アマゾン ウェブ サービスにおける HIPAA セキュリティおよびコンプライアンスのためのアーキテクチャ設計

2018 年 *1* 月

皆様からのフィードバックをお待ちしています。このリンクを使用して、ご意見をお寄せください。

注記

本書は、情報提供のみを目的としています。本書に記載した AWS の製品オファリングと手法は本書の発行時点における内容を表しており、予告なしに変更される場合があります。本書に記載されている情報、および AWS の製品やサービスの使用については、お客様自身の責任で独自に評価していただきます。これらは「現状のまま」提供されるものであり、明示的にも暗黙的にもいかなる保証も提供されません。本書のいかなる内容も、AWS、その関連会社、供給者、またはライセンサーによる保証、表明、契約の責任、条件、保証を意味するものではありません。お客様に対する AWS の責任と義務は、AWS の契約によって制限されます。本書は、AWS とお客様との間の契約の一部ではなく、そのような契約の内容を変更するものでもありません。

目次

はじめに 1

AWS での PHI の暗号化と保護 2

- Amazon EC2 3
- Amazon Systems Manager 3
- Amazon Virtual Private Cloud 4
- Amazon Elastic Block Store 4
- Amazon Redshift 5
- Amazon S3 5
- Amazon S3 Transfer Acceleration 6
- Amazon SNS 6
- Amazon SQS 7
- Amazon Glacier 8
- Amazon RDS for MySQL 8
- Amazon RDS for Oracle 9
- Amazon RDS for PostgreSQL 10
- Amazon RDS for SQL Server 10
- Amazon RDS for MariaDB 12
- Amazon Aurora 12
- Amazon CloudFront 13
- Elastic Load Balancing 14
- Amazon ECS 15
- Amazon EMR 15
- Amazon DynamoDB 16
- Amazon API Gateway 16
- AWS Storage Gateway 17
- AWS KMS を使用した PHI の暗号化 18

AWS Shield 18
AWS Snowball 19
AWS Snowball Edge 20
AWS Snowmobile 20
AWS WAF – ウェブアプリケーションファイアウォール 20
AWS Directory Service 21
Amazon WorkSpaces 21
Amazon WorkDocs 22
Amazon Inspector 23
Amazon Kinesis Streams 23
AWS Lambda 24
AWS Batch 24
Amazon Connect 25
Amazon Route 53 25
AWS CloudHSM 25
Amazon ElastiCache for Redis 26
Amazon CloudWatch 28
Amazon EC2 Container Registry 28
Amazon Macie 28
Amazon QuickSight 29
AWS マネージドサービス 29
AWS Fargate 30
監査、バックアップ、障害復旧 30
文書改訂 33

要約

本書では、米国の医療保険の相互運用性と説明責任に関する法令 (HIPAA) に準拠したアプリケーションを作成するためにアマゾン ウェブ サービス (AWS) を利用する方法について簡単に説明します。保護医療情報 (PHI) の保護を目的とした HIPAA のプライバシールールおよびセキュリティルールについて重点的に取り上げ、データの転送および保管の際に AWS を使用してデータを暗号化する方法を示します。また、監査、バックアップ、障害復旧に関する HIPAA の要件を満たすために AWS の機能を利用する方法についても説明します。

はじめに

1996 年に米国で制定された医療保険の相互運用性と説明責任に関する法令 (HIPAA) は、「対象となる事業体」とその「取引先」に適用されます。対象となる事業体には、特定の電子取引、医療保険、医療情報センターに携わる医療従事者が含まれます。取引先とは、対象となる事業者に対し、保護医療情報 (PHI) へのアクセスが伴うサービスを提供する事業体、ならびに別の取引先のために PHI を作成、受信、保守、または転送する事業体を指します。2009 年に経済的および臨床的健全性のための医療 IT に関する法律 (HITECH) が制定されました。これは、HIPAA の内容を拡張するものです。HIPAA と HITECH により、PHI のセキュリティとプライバシーを保護するための一連の連邦標準が確立されました。HIPAA と HITECH では、PHI の使用と開示、PHI の適切な保護手段、個人の権利、および管理責任に関連する要件を課しています。HIPAA と HITECH について詳しくは、http://www.hhs.gov/ocr/privacy/ をご覧ください。

対象となる事業体やその取引先は、アマゾン ウェブ サービス (AWS) で提供しているセキュアでスケーラブルな低コストの IT コンポーネントを使用することで、HIPAA と HITECH のコンプライアンス要件に準拠したアプリケーションのアーキテクチャを設計できます。AWS が提供する市販のインフラストラクチャプラットフォーム(Commercial-Off-The-Shelf infrastructure platform) は、業界で認められた ISO 27001、FedRAMP などの認証および監査を受けています。Service Organization Control (SOC) レポート (SOC1、SOC2、SOC3) も利用できます。AWS のサービスとデータセンターでは、運用、物理面で何重にもセキュリティ対策を施すことにより、お客様のデータの整合性と安全を確保しています。お支払は実際にご利用になった分だけです。最低料金や、期間を固定した契約は必要ありません。信頼性が高く効率的な AWS は、成長を続ける医療業界に適したソリューションです。

AWS を利用すれば、HIPAA の対象となる事業体とその取引先は、PHI を安全に処理、保管、転送できます。さらに 2013 年 7 月からは、このような目的で AWS をご利用になるお客様に対して、標準化された事業提携契約 (BAA) をご用意しています。

AWS BAA を締結するお客様は、HIPAA アカウントとして指定されたアカウントで、任意の AWS サービスをご利用いただけます。ただし、PHI の処理、保管、転送に使用できるサービスは、AWS BAA で定義されている HIPAA 対応

サービスに限られます。該当するサービスの一覧については、HIPAA 対応サービスのリファレンス ページ (https://aws.amazon.com/compliance/hipaa-eligible-services-reference/) をご覧ください。

AWS では、標準に基づくリスクマネジメントプログラムを継続的に実施して、HIPAA 対応サービスが HIPAA で要件とされている運用面、技術的、物理的な個々の保護手段をサポートすることを確認しています。これらのサービスを使用して PHI を保管、処理、転送することで、お客様と AWS が、AWS ユーティリティベースの運用モデルに適用される HIPAA 要件に対処できます。

AWS 環境上での PHI の暗号化と保護

HIPAA のセキュリティルールには、PHI の転送時および保管時の暗号化に関する要件に対応可能な実装仕様が含まれています。この実装仕様には HIPAA の要件に対応可能ですが、AWS ではお客様に対し、米国保健福祉省 (HHS) によるガイダンス (Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (以降、「ガイダンス」)) に従って、HIPAA 対応サービスを使用して PHI を保管時または転送時に暗号化するよう求めています。このガイダンスは更新される可能性があるため、上記のリンク先のサイトにアクセスしてガイダンスをご覧ください。また、HHS が指定する後継サイト (または関連サイト) でガイダンスが公開される可能性もあります。

AWS には、AWS Key Management Service (AWS KMS) をはじめ、キー管理と PHI の暗号化を容易にし、監査を簡素化する一連の機能とサービスが用意されています。HIPAA コンプライアンス要件に準拠する必要があるお客様は、この包括的な機能とサービスにより、極めて柔軟な方法で PHI の暗号化要件を満たすことができます。

お客様は、暗号化の実装方法を決定する際に、HIPAA 対応サービスに固有の暗号化機能を評価して利用することも、HHS のガイダンスに従った別の方法で暗号化要件を満たすこともできます。以降のセクションでは、HIPAA 対応サービスと別の方法のそれぞれについて、利用できる暗号化機能を使用して PHI を暗号化する方法の概要を示します。また、AWS の KMS を利用して PHI の暗号化に使用するキーを AWS で暗号化する方法についても説明します。

Amazon EC2

Amazon EC2 は、お客様が構成可能なスケーラブルなコンピューティングサービスです。保管時のデータ暗号化にさまざまな方法で対応できます。例えば Amazon EC2 インスタンスでホストされているアプリケーションまたはデータベースプラットフォーム内で PHI を処理する時点で、アプリケーションレベルまたはフィールドレベルで PHI を暗号化するように設定できます。Amazon EC2 でサポートされるデータ暗号化手法は多岐に渡ります。Java や .NET などのアプリケーションフレームワークの標準ライブラリーを使用することも、Microsoft SQL または Oracle の透過的なデータ暗号化機能を使用することもできます。あるいは、他のサードパーティーや SaaS (Software as a Service) ベースのソリューションをアプリケーションに統合することも可能です。また、キーの管理と保管の処理を簡素化するために、Amazon EC2 内で実行するアプリケーションに AWS KMS SDK を統合するという選択肢もあります。さらに、ファイルレベルの暗号化あるいはフルディスク暗号化 (FDE) を使用して保管時のデータ暗号化を実装することもできます。そのためには、AWS Marketplace パートナーのサードパーティー製ソフトウェアやネイティブファイルシステム暗号化ツール (dm-crypt、LUKS など) を利用します。

PHI が含まれるネットワークトラフィックの場合、転送中のデータを暗号化しなければなりません。外部ソース (インターネットや従来の IT 環境など) と Amazon EC2 間のトラフィックには、ガイダンスに従った業界標準の転送時の暗号化メカニズム (TLS、IPsec など) を使用する必要があります。Amazon Virtual Private Cloud (VPC) の内部では、Amazon EC2 インスタンス間でデータが送受信されます。このような場合でも、PHI が含まれるネットワークトラフィックは暗号化する必要があります。データを転送時に暗号化する TLS やその他のプロトコルをサポートするアプリケーションであれば、ほとんどの場合、ガイダンスに準拠した構成にできます。暗号化をサポートしていないアプリケーションやプロトコルについては、IPsec などの実装を使用した暗号化トンネルを介して、PHI を転送するセッションをインスタンス間でやり取りできます。

Amazon Systems Manager

AWS Systems Manager のコンソールとリソースグループは、HIPAA BAA の適用対象ではありません。

AWS Systems Manager (旧称 Amazon EC2 Systems Manager) は、AWS リソース全体の運用データの一元管理、タスクの自動化を容易にする統合インター

フェイスです。インフラストラクチャ内の運用上の問題を検出して解決するまでの時間が短縮されます。Systems Manager では、インフラストラクチャのパフォーマンスと構成の全体像を把握できるため、リソースとアプリケーションの管理が簡素化され、大規模なインフラストラクチャを簡単に運用、管理できます。

PHI が含まれる可能性のあるデータを Amazon S3 などの他のサービスに出力する際は、PHI の保管に関する受信側サービスのガイダンスに従う必要があります。例えば、文書名、パラメータ名などといったメタデータや識別子には、PHI を含めないでください。また、リソースグループコンソールや AWS Systems Manager コンソールの使用は避ける必要があります。ただし、EC2 Systems Manager のコンソールは使用できます。

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud (VPC) には、HIPAA 準拠のためのアーキテクチャ設計に忠実に従った一連のネットワークセキュリティ機能が用意されています。例えば、ステートレスなネットワークアクセス制御リスト、ステートフルなセキュリティグループへの動的インスタンス再割り当てなどといった機能を使用すれば、柔軟な方法で、不正なネットワークアクセスからインスタンスを保護できます。Amazon VPC では、お客様独自のネットワークアドレス空間を AWS に拡張できるだけでなく、データセンターをさまざまな方法で AWS に接続できるようになっています。PHI を処理、転送、または保管するインスタンスへの接続については、接続が許可されたかどうかを示す監査証跡が VPC フローログに記録されます。Amazon VPC について詳しくは、http://aws.amazon.com/vpc/ をご覧ください。

Amazon Elastic Block Store

Amazon EBS での保管時のデータ暗号化は、本ホワイトペーパーの公開時点で効力のあるガイダンスに従っています。このガイダンスは更新される可能性があるため、Amazon EBS の暗号化を継続的に評価して、お客様のコンプライアンス要件と規制上の要件を満たしているかどうかを判断してください。
Amazon EBS の暗号化では、EBS ボリュームごとに固有のボリューム暗号化キーが生成されます。各ボリュームキーの暗号化に使用するマスターキーは、AWS Key Management Service で柔軟に選択することができます。詳しくは、http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html をご覧ください。

Amazon Redshift

Amazon Redshift のクラスターでは、データベース暗号化を使用して保管中のデータを保護できます。クラスターに対して暗号化を有効にすると、ハードウェアアクセラレーション対応の高度暗号化規格 (AES) による 256 ビットの対称キーを使用して、バックアップを含むすべてのデータが暗号化されます。Amazon Redshift で採用している暗号化アーキテクチャは、4 重のキーをベースとしています。具体的には、データ暗号化キー、データベースキー、クラスターキー、マスターキーの 4 つです。Amazon Redshift クラスターのデータベースキーは、クラスターキーによって暗号化されます。クラスターキーを管理するには、AWS KMS または AWS CloudHSM (Hardware Security Module) のいずれかを使用します。Amazon Redshift での保管時のデータ暗号化は、本ホワイトペーパーの公開時点で効力のあるガイダンスに従っています。このガイダンスは更新される可能性があるため、Amazon Redshift の暗号化を継続的に評価して、お客様のコンプライアンス要件と規制上の要件を満たしているかどうかを判断してください。詳しくは、http://docs.aws.amazon.com/redshift/latest/mgmt/working-with-db-encryption.html をご覧ください。

PHI を格納する Amazon Redshift への接続には、転送時の暗号化が使用されていなければなりません。設定を評価して、ガイダンスに従っていることを確認してください。詳しくは、http://docs.aws.amazon.com/redshift/latest/mgmt/connecting-ssl-support.html をご覧ください。

Amazon Redshift Spectrum を使用することにより、Amazon S3 内のエクサバイト規模のデータに対して Redshift SQL クエリを実行できるようになります。Redshift Spectrum は Amazon Redshift の機能であるため、同じく HIPAA BAA の適用対象となります。

Amazon S3

Amazon S3 を使用する場合、保存データを暗号化する方法として、サーバー側の暗号化とクライアント側の暗号化を使用できます。キーの管理方法にも複数のオプションがあります。詳しくは、http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html をご覧ください。

PHI を格納する Amazon S3 への接続には、暗号化された転送 (HTTPS) を受け入れるエンドポイントが使用されていなければなりません。リージョンごとのエンドポイントのリストについては、http://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region をご覧ください。

バケット名、オブジェクト名、メタデータには、PHI を含めないでください。これらのデータには S3 のサーバー側の暗号化が適用されず、通常はクライアント側の暗号化アーキテクチャで暗号化されることもありません。

Amazon S3 Transfer Acceleration

Amazon S3 Transfer Acceleration (S3TA) を使用すると、クライアントと遠く離れた S3 バケットとの間で、セキュアな高速ファイル転送を簡単に実現できます。Transfer Acceleration では、世界中に分散された Amazon CloudFront のエッジロケーションを利用します。エッジロケーションに到着したデータは、最適化されたネットワークパスで Amazon S3 にルーティングされます。

AWS S3 TA を使用して転送される、PHI が含まれるデータについては、必ず転送時および保管時に暗号化されるようにしてください。利用可能な暗号化オプションについては、Amazon S3 のガイダンスをご覧ください。

Amazon SNS

保護医療情報 (PHI) で Amazon Simple Notification Service (SNS) を使用する場合、理解しておかなければならない重要な暗号化要件があります。それは、各 AWS リージョンで SNS 提供の HTTPS API エンドポイントを使用しなければならないことです。HTTPS エンドポイントでは AWS に送信されるデータのプライバシーと整合性を保護するために、暗号化された接続を使用します。HTTPS API エンドポイントを網羅したリストについては、http://docs.aws.amazon.com/general/latest/gr/rande.html#sns_region をご覧ください。

さらに、Amazon SNS には CloudTrail サービスも統合されています。このサービスは、お客様の AWS アカウントで Amazon SNS コンソールまたは Amazon SNS API を使用して行われた API 呼び出しの情報を収集し、そのログファイルを指定の Amazon S3 バケットに配信します。CloudTrail によって収集された情報を基に、Amazon SNS に対して行われたリクエストの送信元 IP アドレス、リクエストの実行者、リクエストが行われた日時などの詳細を特定できま

す。SNS 操作のロギングについて詳しくは、http://docs.aws.amazon.com/sns/latest/dg/logging-using-cloudtrail.html をご覧ください。

Amazon SQS

Amazon SQS で保護医療情報 (PHI) を扱うためには、次のキー暗号化の要件があります。

- クエリリクエストを介した Amazon SQS Queue との通信は、HTTPS を使用して暗号化する必要があります。詳しくは、http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/MakingRequests_MakingQueryRequestsArticle.html をご覧ください。
- Amazon SQS では、AWS Key Management Service (AWS KMS) に統合されたサーバー側の暗号化により、保管中のデータが保護されます。サーバー側の暗号化を追加すると、暗号化されたキューを使用できるようになるため、機密データを送受信する際のセキュリティが強化されます。Amazon SQS のサーバー側の暗号化では、256 ビットの高度な暗号化規格 (AES-256 GCM アルゴリズム) を使用して各メッセージの本文が暗号化されます。AWS KMS を統合することにより、Amazon SQS メッセージを保護するキーと他の AWS リソースを保護するキーを一元管理できます。暗号化キーの使用情報が AWS CloudTrail に逐一記録されるため、法規制およびコンプライアンスの要件を満たすことができます。詳細およびお客様のリージョンで Amazon SQS のサーバー側の暗号化 (SSE) を利用できるかどうかについては、http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-server-side-encryption.html をご覧ください。
- サーバー側の暗号化を使用しない場合は、メッセージのペイロード自体を暗号化してから SOS に送信する必要があります。メッセージのペイロードを暗号化する方法としては、Amazon SQS 拡張クライアントと Amazon S3 暗号化クライアントを併せて使用する方法があります。クライアント側の暗号化の使用方法について詳しくは、https://aws.amazon.com/blogs/developer/encrypting-message-payloads-using-the-amazon-sqs-extended-client-and-the-amazon-s3-encryption-client/ をご覧ください。

Amazon SQS には CloudTrail サービスも統合されています。このサービスは、お客様の AWS アカウントで Amazon SQS コンソールまたは Amazon SQS API を使用して行われた API 呼び出しの情報を収集し、そのログファイルを指定の Amazon S3 バケットに配信します。CloudTrail によって収集された情報を基に、Amazon SQS に対して行われたリクエストの送信元 IP アドレス、リクエストの実行者、リクエストが行われた日時などの詳細を特定できます。SQS 操作のロギングについて詳しくは、http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/logging-using-cloudtrail.html をご覧ください。

Amazon Glacier

Amazon Glacier では、AES による 256 ビットの対称キーを使用して保存データが自動的に暗号化されます。セキュアなプロトコルによるセキュアなデータ転送がサポートされます。

PHI を格納する Amazon Glacier への接続には、暗号化された転送 (HTTPS) を受け入れるエンドポイントが使用されていなければなりません。リージョンごとのエンドポイントのリストについては、http://docs.aws.amazon.com/general/latest/gr/rande.html#glacier_region をご覧ください。

アーカイブ名、ボールト名、メタデータには、PHI を含めないでください。これらのデータには Amazon Glacier のサーバー側の暗号化が適用されず、通常はクライアント側の暗号化アーキテクチャで暗号化されることもありません。

Amazon RDS for MySQL

Amazon RDS for MySQL では、AWS KMS によって管理されるキーを使用して、MySQL データベースを暗号化できます。Amazon RDS 暗号化を使用して実行されているデータベースインスタンスでは、基盤となるストレージ内の保存データは、本ホワイトペーパーの公開時点で効力のあるガイダンスに従って暗号化されます。また、自動バックアップ、リードレプリカ、スナップショットについても同じく暗号化されます。このガイダンスは更新される可能性があるため、Amazon RDS for MySQL の暗号化を継続的に評価して、お客様のコンプライアンス要件と規制上の要件を満たしているかどうかを判断してください。Amazon RDS での保存データの暗号化について詳しくは、http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html をご覧ください。

PHI を格納する RDS for MySQL への接続には、転送時の暗号化が使用されていなければなりません。暗号化された接続を使用する方法について詳しくは、http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html をご覧ください。

Amazon RDS for Oracle

Amazon RDS for Oracle を使用すると、保存する PHI をさまざまな方法で暗号化できます。

AWS KMS によって管理されるキーを使用して、Oracle データベースを暗号化できます。Amazon RDS 暗号化を使用して実行されているデータベースインスタンスでは、基盤となるストレージ内の保存データは、本ホワイトペーパーの公開時点で効力のあるガイダンスに従って暗号化されます。また、自動バックアップ、リードレプリカ、スナップショットについても同じく暗号化されます。このガイダンスは更新される可能性があるため、Amazon RDS for Oracle の暗号化を継続的に評価して、お客様のコンプライアンス要件と規制上の要件を満たしているかどうかを判断してください。Amazon RDS での保存データの暗号化について詳しくは、http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html をご覧ください。

また、Oracle の透過的データベース暗号化 (TDE) を使用することもできますが、設定を評価して、ガイダンスに従っていることを確認してください。Oracle TDE は、Oracle Enterprise Edition で使用可能な Oracle Advanced Security オプションの機能です。この機能により、ストレージに書き込む前にデータが自動的に暗号化され、ストレージから読み取る際にデータが自動的に暗号化解除されます。AWS CloudHSM を使用して、Amazon RDS の Oracle TDE キーを保管することもできます。詳しくは、以下のリソースをご覧ください。

- Amazon RDS for Oracle の透過的データベース暗号化については、http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.Oracle.Options.AdvSecurity.html をご覧ください。
- AWS CloudHSM を使用して Amazon RDS の Oracle TDE キーを保管する方法については、http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.OracleCloudHSM.html をご覧ください。

PHI を格納する Amazon RDS for Oracle への接続には、転送時の暗号化が使用されていなければなりません。設定を評価して、ガイダンスに従っていることを確認してください。転送時の暗号化に対応するには、Oracle ネイティブのネットワーク暗号化機能を使用し、Amazon RDS for Oracle のオプションでこの機能を有効にします。詳しくは、http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.Oracle.Options.NetworkEncryption.html をご覧ください。

Amazon RDS for PostgreSQL

Amazon RDS for PostgreSQL では、AWS KMS によって管理されるキーを使用して、PostgreSQL データベースを暗号化できます。Amazon RDS 暗号化を使用して実行されているデータベースインスタンスでは、基盤となるストレージ内の保存データは、本ホワイトペーパーの公開時点で効力のあるガイダンスに従って暗号化されます。また、自動バックアップ、リードレプリカ、スナップショットについても同じく暗号化されます。このガイダンスは更新される可能性があるため、Amazon RDS for PostgreSQL の暗号化を継続的に評価して、お客様のコンプライアンス要件と規制上の要件を満たしているかどうかを判断してください。Amazon RDS での保存データの暗号化について詳しくは、http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html をご覧ください。

PHI を格納する RDS for PostgreSQL への接続には、転送時の暗号化が使用されていなければなりません。暗号化された接続を使用する方法について詳しくは、http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html をご覧ください。

Amazon RDS for SQL Server

次の RDS for SQL Server で、PHI の保管がサポートされます。

- 2008 R2 - Enterprise Edition のみ
- 2012、2014、2016 - Web Edition、Standard Edition、Enterprise Edition

重要: SQL Server Express Edition はサポートされていないため、PHI のストレージとして使用しないでください。

PHI を保管するには、保存データを暗号化するようにインスタンスで設定し、転送時の暗号化と監査を有効にする必要があります。以下で詳しく説明します。

保管時の暗号化

AWS KMS によって管理されるキーを使用して、SQL Server データベースを暗号化できます。Amazon RDS 暗号化を使用して実行されているデータベースインスタンスでは、基盤となるストレージ内の保存データは、本ホワイトペーパーの公開時点で効力のあるガイダンスに従って暗号化されます。また、自動バックアップ、スナップショットについても同じく暗号化されます。このガイダンスは更新される可能性があるため、Amazon RDS for SQL Server の暗号化を継続的に評価して、お客様のコンプライアンス要件と規制上の要件を満たしているかどうかを判断してください。Amazon RDS での保存データの暗号化について詳しくは、
http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html をご覧ください。

SQL Server Enterprise Edition を使用している場合は、サーバーの透過的データ暗号化 (TDE) を代わりに使用することもできます。この機能により、ストレージに書き込む前にデータが自動的に暗号化され、ストレージから読み取る際にデータが自動的に暗号化解除されます。RDS for SQL Server の透過的データ暗号化について詳しくは、

http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.SQLServer.Options.TDE.html をご覧ください。

転送時の暗号化

PHI を格納する Amazon RDS for SQL Server への接続では、SQL Server で SSL を強制して転送時の暗号化を有効にする必要があります。SSL の強制を有効にするには、Amazon RDS SQL Server のパラメータグループのパラメータを使用します。RDS for SQL Server での SSL の強制について詳しくは、

http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/SQLServer.Concepts.General.SSL.Using.html をご覧ください。

監査

PHI を格納する RDS for SQL Server インスタンスでは、監査を有効にする必要があります。監査を有効にするには、Amazon RDS SQL Server のパラメータグループのパラメータを使用します。RDS for SQL Server の監査について詳しくは、http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_SQLServer.html#SQLServer.Concepts.General.Compliance をご覧ください。

Amazon RDS for MariaDB

Amazon RDS for MariaDB では、AWS KMS によって管理されるキーを使用して、MariaDB データベースを暗号化できます。Amazon RDS 暗号化を使用して実行されているデータベースインスタンスでは、基盤となるストレージ内の保存データは、本ホワイトペーパーの公開時点で効力のあるガイダンスに従って暗号化されます。また、自動バックアップ、リードレプリカ、スナップショットについても同じく暗号化されます。このガイダンスは更新される可能性があるため、Amazon RDS for MariaDB の暗号化を継続的に評価して、お客様のコンプライアンス要件と規制上の要件を満たしているかどうかを判断してください。Amazon RDS での保存データの暗号化について詳しくは、http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html をご覧ください。

PHI を格納する RDS for MariaDB への接続には、転送時の暗号化が使用されていなければなりません。暗号化された接続を有効にする方法について詳しくは、http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html をご覧ください。

Amazon Aurora

Amazon Aurora では、AWS KMS によって管理されるキーを使用して、Aurora データベースを暗号化できます。Amazon Aurora 暗号化を使用して実行されているデータベースインスタンスでは、基盤となるストレージ内の保存データは、本ホワイトペーパーの公開時点で効力のあるガイダンスに従って暗号化さ

れます。また、自動バックアップ、リードレプリカ、スナップショットについても同じく暗号化されます。このガイダンスは更新される可能性があるため、Amazon Aurora の暗号化を継続的に評価して、お客様のコンプライアンス要件と規制上の要件を満たしているかどうかを判断してください。Amazon RDS での保存データの暗号化について詳しくは、http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html をご覧ください。

BAA 、Amazon Aurora の MySQL 対応エディションまたは PostgreSQL 対応エディションのいずれかを使用できます。

PHI を格納する Aurora への接続には、転送時の暗号化が使用されていなければなりません。暗号化された接続を有効にする方法について詳しくは、http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html をご覧ください。

Amazon CloudFront

Amazon CloudFront は、ウェブサイト、API、動画コンテンツその他のウェブアセットの配信を加速するグローバルコンテンツ配信ネットワーク (CDN) サービスです。Amazon CloudFront はアマゾン ウェブ サービスの他の製品と統合されているため、エンドユーザーへのコンテンツの高速配信を簡単に行うことができます。固定基本料金なしでご利用いただけます。

CloudFront で転送される PHI が 確実に暗号化されるようにするには、発信元から閲覧者までの全経路で HTTPS を使用するように CloudFront を設定しなければなりません。これには、CloudFront と閲覧者との間のトラフィック、カスタム発信元からの再配信、S3 からの配信も含まれます。

CloudFront にキャッシュされている間、暗号化された状態でデータが保管されるように、発信元でデータを暗号化する必要があります。S3 を発信元として使用する場合は、S3 のサーバー側の暗号化機能を利用できます。一方、カスタム発信元から配信する場合は、その発信元でデータが暗号化されるようにする必要があります。

Lambda@Edge

Lambda@Edge は、AWS エッジロケーションで Lambda 関数の実行を可能にするコンピューティングサービスです。CloudFront を介して配信するコンテン

ツをカスタマイズする際に使用できます。PHI で Lambda@Edge を使用する場合、CloudFront の使用に関するガイダンス従う必要があります。Lambda@Edge への接続および Lambda@Edge からの接続はすべて、HTTPS または SSL/TLS を使用して暗号化してください。

Elastic Load Balancing

PHI が含まれるセッションの終端と処理に Elastic Load Balancing を使用できます。このサービスでは、ロードバランサーとして、Classic Load Balancer または Application Load Balancer を選択できます。PHI が含まれるすべてのネットワークトラフィックは、発信元から宛先までの全経路で、暗号化された状態で転送される必要があります。このため、2 種類のアーキテクチャを柔軟に実装できるようになっています。

1 つは、暗号化プロトコルを使用して接続するロードバランサーを作成して、Elastic Load Balancing で HTTPS、HTTP/2 over TLS (アプリケーションの場合)、または SSL/TLS を終端する方法です。この場合、ロードバランサーと HTTPS、HTTP/2 over TLS、または SSL/TLS セッションを開始したクライアントとの間のトラフィックを暗号化できます。PHI が含まれるセッションでは、転送時の暗号化に対応するために、フロントエンドとバックエンド両方のリスナーを暗号化する必要があります。証明書およびセッションネゴシエーションポリシーを評価して、ガイダンスに従った状態に維持してください。詳しくは、http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-https-load-balancers.html をご覧ください。

もう 1 つは、基本 TCP モード (Classic の場合) または WebSocket (Application Load Balancer の場合) を使用して Amazon ELB を設定し、暗号化セッションをバックエンドのインスタンスにパススルーして、そこでセッションを終端する方法です。このアーキテクチャでは、お客様独自のインスタンス内で実行されるアプリケーションで、お客様が独自の証明書と TLS ネゴシエーションポリシーを管理します。詳しくは、http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-listener-config.html をご覧ください。

いずれのアーキテクチャでも、お客様が HIPAA と HITECH の要件に一致すると判断したレベルのロギングを実装する必要があります。

Amazon ECS

Amazon EC2 Container Service (ECS) は、Docker コンテナをサポートする、優れたスケーラビリティとパフォーマンスを備えたコンテナ管理サービスです。このサービスを使用すると、Amazon EC2 インスタンスの管理対象クラスター上のアプリケーションを簡単に実行できます。Amazon ECS を使用すれば、独自のクラスター管理インフラストラクチャをインストール、運用、拡張する必要がありません。さらに、単純な API 呼び出しを使用して、Docker 対応のアプリケーションを起動、停止したり、クラスター全体の状態のクエリを実行したり、使い慣れた多数の機能 (セキュリティグループ、Elastic Load Balancing、EBS ボリューム、IAM ロールなど) にアクセスしたりできます。Amazon ECS を使用して、リソースの需要や可用性の要件に応じてクラスター内のコンテナの配置をスケジュールできます。

PHI を処理するワークロードで ECS を使用するために、追加設定は不要です。ECS は、オーケストレーションサービスとして機能して EC2 内のコンテナ (コンテナのイメージは S3 内に保管される) の起動を制御するオーケストレーションサービスとして機能します。ECS は、オーケストレーション対象のワークフロー内のデータを使用することも、これらのデータに依存することもありません。HIPAA の規制と AWS 事業提携契約 (BAA) に従い、ECS で起動されたコンテナがアクセスする PHI は、転送時および保管時に暗号化する必要があります。AWS のストレージオプション (S3、EBS、KMS など) ごとに、保存データの暗号化には、さまざまなメカニズムを利用できます。コンテナ間で送信される PHI が全経路で暗号化されるようにするために、オーバーレイネットワーク (VNS3、Weave Net など) を実装して追加の暗号化層を設けることもあります。そのような場合でも、(CloudTrail などを使用して) ロギングを有効にして、すべてのコンテナのログが CloudWatch に転送されるようにしてください。

Amazon EMR

Amazon EMR では、Amazon EC2 インスタンスのクラスターをお客様のアカウントとしてデプロイして管理します。

Amazon EMR での暗号化については、https://docs.aws.amazon.com/ElasticMapReduce/latest/ReleaseGuide/emr-data-encryption-options.html をご覧ください。

Amazon DynamoDB

PHI を格納する Amazon DynamoDB への接続には、暗号化された転送 (HTTPS) を受け入れるエンドポイントが使用されていなければなりません。リージョンごとのエンドポイントのリストについては、http://docs.aws.amazon.com/general/latest/gr/rande.html#ddb_region をご覧ください。

Amazon DynamoDB に保管する PHI は、ガイダンスに従って暗号化して保管する必要があります。Amazon DynamoDB をご利用のお客様は、任意のアプリケーション開発フレームワークを使用してアプリケーション内で PHI を暗号化してから、Amazon DynamoDB に保管できます。あるいは、AWS Labs GitHub リポジトリに用意されている、コンテンツ暗号化のためのクライアント側のライブラリを使用することもできます。この実装を評価して、ガイダンスに従っていること確認してください。ガイダンスに従うには、この実装を評価する価値があります。詳しくは、https://github.com/awslabs/aws-dynamodb-encryption-java をご覧ください。基本キーを選択する際およびインデックスを作成する際は、Amazon DynamoDB でのクエリやスキャンに非セキュアな PHI が必要となることがないように十分に注意してください。

Amazon API Gateway

Amazon API Gateway は、PHI の処理と転送に利用できます。転送時の暗号化には自動的に HTTPS エンドポイントが使用されますが、ペイロードをクライアント側で暗号化することもできます。API Gateway では、キャッシュされていないすべてのデータはメモリ経由で渡され、ディスクへの書き込みは行われません。API Gateway での権限付与には、AWS の署名バージョン 4 を使用できます。詳しくは、以下のリソースをご覧ください。

- https://aws.amazon.com/api-gateway/faqs/#security
- https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-control-access-to-api.html

任意のサービスを統合して API Gateway に接続できます。ただし、PHI が関与する場合は、そのサービスがガイダンスと BAA に従って設定されている必要があります。API Gateway とバックエンドのサービスとの統合については、https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-method-settings.html をご覧ください。

AWS CloudTrail と Amazon CloudWatch を併せて使用することで、お客様のロギング要件に合わせてログを記録できます。API Gateway を介して (ヘッダー、URL、リクエスト/レスポンスで) 送信される PHI は、ガイダンスに従って設定された HIPAA 対応サービスのみで収集されるようにしてください。API Gateway でのロギングについて詳しくは、https://aws.amazon.com/premiumsupport/knowledge-center/api-gateway-cloudwatch-logs/ をご覧ください。

AWS Storage Gateway

AWS Storage Gateway は、オンプレミスアプリケーションから AWS クラウドストレージをシームレスに利用できるようにするハイブリッドストレージサービスです。既存のストレージアプリケーションとワークフローは、業界標準のストレージプロトコルを使用して AWS クラウドストレージサービスに接続されます。このため、プロセスの中断を最小限に抑えることができます。

ファイルゲートウェイ

Amazon S3 へのファイルインターフェイスをサポートするタイプの AWS Storage Gateway は、ファイルゲートウェイと呼ばれます。ファイルゲートウェイは、現行のブロックベースのボリュームと VTL ストレージに追加されます。ファイルゲートウェイでは HTTP を使用して S3 と通信し、すべてのオブジェクトを暗号化して保管します。これに対し、S3 では SSE-S3 (デフォルト) またはクライアント側の暗号化を使用してキーを AWS KMS に保管します。ファイル名などのファイルメタデータは暗号化されないため、ファイルメタデータには PHI を含めないでください。

ボリュームゲートウェイ

ボリュームゲートウェイでは、オンプレミスアプリケーションサーバーから iSCSI (Internet Small Computer System Interface) デバイスとしてマウントできる、クラウドベースのストレージボリュームがサポートされます。ボリュームゲートウェイ VM には、社内のコンプライアンス要件と規制上の要件に従って、ローカルディスクをアップロードバッファーおよびキャッシュとして接続します。PHI の場合、ローカルディスクには、保管時の暗号化に対応できるものを使用することが推奨されます。転送中の PHI を保護するために、ボリュームゲートウェイ VM と AWS 間の通信は SSL (TLS 1.2) を使用して暗号化されます。

テープゲートウェイ

テープゲートウェイは、オンプレミスで実行されるサードパーティー製バックアップアプリケーションとの VTL (仮想テープライブラリ) インターフェイスを提供します。テープバックアップジョブをセットアップする際は、サードパーティー製バックアップアプリケーション内で PHI の暗号化を有効にしてください。転送中の PHI を保護するために、テープゲートウェイ VM と AWS 間の通信は SSL (TLS 1.2) を使用して暗号化されます。

PHI でいずれかの Storage Gateway 構成を使用する場合は、詳細なロギングを有効にする必要があります。詳しくは、http://docs.aws.amazon.com/storagegateway/latest/userguide/logging-using-cloudtrail-common.html をご覧ください。

AWS KMS を使用した PHI の暗号化

お客様のアプリケーション内、または AWS KMS が統合された AWS サービス内で PHI を暗号化するために使用するデータ暗号化キーを、AWS KMS のマスターキーを使って暗号化/暗号化解除できます。お客様のアプリケーション内、または AWS KMS が統合された AWS サービス内で PHI を暗号化できます。AWS KMS は HIPAA アカウントと連動させることができますが、PHI を処理、保管、転送できるのは、HIPAA 対応サービスに限られます。AWS KMS は一般に、他の HIPAA 対応サービスで実行されるアプリケーション用のキーを生成、管理するために使用されます。例えば、Amazon EC2 内で PHI を処理するアプリケーションでは、GenerateDataKey API 呼び出しを使用して、そのアプリケーション内で PHI を暗号化および暗号化解除するためのデータ暗号化キーを生成できます。このデータ暗号化キーは、AWS KMS に保管されているお客様のマスターキーで保護できます。AWS KMS に対する API 呼び出しは AWS CloudTrail のログに記録されることから、監査性の極めて高いが生成されます。ただし、AWS KMS に保管されるキーのタグ (メタデータ) には、PHI を格納しないでください。

AWS Shield

AWS Shield は、AWS で実行しているウェブアプリケーションを分散型 DoS 攻撃 (DDoS) から保護する、マネージド型の保護サービスです。AWS Shield では、アプリケーションのダウンタイムとレイテンシーを最小限に抑えるため

に、常時稼働の検出機能と自動インライン緩和機能を提供します。そのため、AWS サポートに頼らなくても、DDoS 攻撃に対する保護が得られます。

AWS Shield は PHI の保管と転送には使用できませんが、PHI を扱うウェブアプリケーションの保護手段として利用できます。そのため、AWS Shield を使用するために特別な設定は必要ありません。

AWS をご利用のすべてのお客様は、追加料金なしで AWS Shield Standard の自動保護を利用できます。AWS Shield Standard は、発生しがちなネットワーク層とトランスポート層に対する DDoS 攻撃からの保護を提供します。この攻撃はウェブサイトやアプリケーションを標的としたものです。Elastic Load Balancing (ELB)、Amazon CloudFront、および Amazon Route 53 リソースで実行されるウェブアプリケーションを標的とした攻撃に対するさらに高度なレベルの保護をご希望の場合は、AWS Shield Advanced にサブスクライブできます。

AWS Snowball

AWS Snowball (Snowball) を使用すると、数百テラバイトまたはペタバイト規模の大容量データをオンプレミスのデータセンターと Amazon Simple Storage Service (Amazon S3) との間で転送することができます。

AWS Snowball に格納する PHI は、ガイダンスに従って保管時に暗号化しなければなりません。重要なジョブを作成する際は、AWS Key Management Service (AWS KMS) マスターキーの ARN を指定して Snowball 内のデータを保護する必要があります。さらに、インポートジョブの作成時には、ガイダンスで規定されている暗号化基準を満たす宛先 S3 バケットを選択する必要があります。現在、Snowball では AWS KMS で管理されたキー (SSE-KMS) によるサーバー側の暗号化も、お客様提供のキー (SSE-C) によるクライアント側の暗号化もサポートしていません。Amazon S3 で管理された暗号化キー (SSE-S3) を使用したサーバー側の暗号化はサポートしています。詳しくは、Protecting Data Using Server-Side Encryption with Amazon S3- Managed Encryption Keys (SSE-S3) をご覧ください。

別の方法として、任意の暗号化方法を使用して PHI を暗号化した上で、データを AWS Snowball に保管することもできます。

現在、BAA の一環として標準の AWS Snowball アプライアンスまたは AWS Snowmobile をご利用いただけます。

AWS Snowball Edge

AWS Snowball Edge では、標準のストレージインターフェイスを使用して既存のアプリケーションとインフラストラクチャに接続し、データ転送プロセスを効率化します。設定と統合は簡単です。Snowball Edge をクラスター化してローカルのストレージ層を形成し、オンプレミスでデータを処理できるため、クラウドにアクセスできない時でもアプリケーションを実行し続けることができます。

Snowball Edge の使用時に PHI が暗号化された状態を維持する必要があります。このためには、AWS Greengrass によって実行される AWS Lambda プロシージャの使用時に、Snowball Edge と外部のリソースとの間で PHI をやり取りする際に HTTPS や SSL/TLS などの暗号化された接続プロトコルが使用されるようにします。さらに、Snowball Edge のローカルボリュームに保管中の PHI は、ローカルアクセスの場合も NFS の場合も暗号化されている必要があります。マネジメントコンソールおよび S3 への一括転送用 API を使用する場合、Snowball Edge に格納されるデータは自動的に暗号化されます。S3 へのデータ転送について詳しくは、前述の AWS Snowball 関連のガイダンスをご覧ください。

AWS Snowmobile

Snowmobile は AWS マネージドサービスとして運用されるため、AWS からお客様に連絡して、デプロイの要件を判断し、ネットワーク接続を手配するとともにデータ移行を支援することになります。Snowmobile に保管されるデータは、AWS Snowball と同様のガイダンスに従って暗号化されます。

AWS WAF – ウェブアプリケーションファイアウォール

よくある脆弱性を突くエクスプロイトは、アプリケーションの可用性に影響を与えたり、セキュリティの侵害やリソースの過剰な消費を引き起こす可能性があります。AWS WAF は、このようなエクスプロイトからお客様のウェブアプリケーションを保護するウェブアプリケーションファイアウォールです。

AWS WAF は、AWS 上でホストされている、PHI を操作または交換するウェブアプリケーションと、エンドユーザーとの間に配置できます。PHI を転送す

る場合の例に漏れず、AWS 上では、PHI を含むデータを転送する際に暗号化する必要があります。利用可能な暗号化オプションについて詳しくは、Amazon EC2 に関するガイダンスをご覧ください。

AWS Directory Service

AWS Directory Service for Microsoft AD

AWS Directory Service for Microsoft Active Directory (Enterprise Edition) は AWS Microsoft AD とも呼ばれ、これを使用すると、AWS クラウド内のマネージド型 Active Directory をディレクトリ対応型ワークロードと AWS リソースで使用できるようになります。AWS Microsoft AD では、ディレクトリの内容 (PHI が格納されたものを含む) を、AWS が管理する暗号化キーを使用して暗号化された Amazon Elastic Block Store ボリュームに直接保管します。詳しくは、「Amazon EBS Encryption」をご覧ください。Active Directory クライアントとの間で転送されるデータは、Amazon Virtual Private Cloud (VPC) ネットワークに送信される時点で、Lightweight Directory Access Protocol (LDAP) を使用して暗号化されます。Active Directory クライアントがオンプレミスネットワーク内に常駐している場合、トラフィックは仮想プライベートネットワークのリンクまたは AWS Direct Connect のリンクによって VPC に送信されます。

Amazon Cloud Directory

Amazon Cloud Directory では、柔軟性に優れたクラウドネイティブのディレクトリを構築し、複数のディメンションにまたがるデータの階層を編成できます。Cloud Directory を使用して、組織図、コースカタログ、デバイスレジストリなどといった各種ユースケースのディレクトリを作成することもできます。例えば、報告体制、所在地、コストセンターのそれぞれに対応する階層内を検索できる組織図を作成できます。Amazon Cloud Directory は、AWS Key Management Service (KMS) で管理される 256 ビットの暗号化キーを使用して、データを保管時および転送時に自動的に暗号化します。

Amazon WorkSpaces

Amazon WorkSpaces は、AWS で稼働する完全マネージド型のセキュアな DaaS (Desktop-as-a-Service) ソリューションです。Amazon WorkSpaces を使用すると、クラウドベースの Microsoft Windows 仮想デスクトップを簡単にプロビジョニングできます。ユーザーは、サポート対象の任意のデバイスを使っ

て、必要な文書、アプリケーション、リソースにいつでもどこからでもアクセスできます。

Amazon WorkSpaces のデータの保管場所は、Amazon Elastic Block Store ボリュームです。WorkSpaces のストレージボリュームは、AWS Key Management Service で管理されるキーを使用して暗号化できます。WorkSpace で暗号化を有効にすると、基盤となるストレージに保管されるデータとディスクストレージの自動バックアップに含まれるデータの両方が、ガイダンスに従った方法で保管時に暗号化されます。WorkSpace クライアントから WorkSpace への通信は、業界標準の SSL によって保護されます。Amazon WorkSpaces を使用した保管時のデータ暗号化について詳しくは、http://docs.aws.amazon.com/workspaces/latest/adminguide/encrypt-workspaces.html をご覧ください。

Amazon WorkDocs

Amazon WorkDocs は、完全マネージド型のセキュアなエンタープライズファイルストレージおよび共有サービスであり、ユーザーの生産性を向上させる高度な管理機能とフィードバック機能を備えています。

Amazon WorkDocs のファイルは、保存時に、AWS Key Management Service (KMS) で管理されるキーを使って暗号化されます。また、すべてのデータは転送時に、業界標準の SSL を使用して暗号化されます。AWS のウェブおよびモバイルアプリケーションとデスクトップ同期クライアントは、SSL を使用して Amazon WorkDocs にファイルを直接送信します。WorkDocs 管理者は Amazon WorkDocs マネジメントコンソールを使用して監査ログを表示し、ファイルおよびユーザーアクティビティを時間で追跡したり、ユーザーに組織外部のユーザーとのファイル共有を許可するかどうかを選択したりできます。Amazon WorkDocs には CloudTrail サービスも統合されています。このサービスは、お客様の AWS アカウントで Amazon WorkDocs コンソールまたは Amazon WorkDocs API を使用して行われた API 呼び出しの情報を収集し、そのログファイルを指定の Amazon S3 バケットに配信します。

RADIUS サーバーを使用した多要素認証 (MFA) を利用して、認証プロセスに追加のセキュリティ層を適用することもできます。この場合、ユーザーはログインする際に、ユーザー名とパスワードを入力し、さらにハードウェアまたはソフトウェアトークンから提供された OTP (ワンタイムパスワード) を入力することになります。

詳しくは、以下のリソースをご覧ください。

- https://aws.amazon.com/workdocs/details/#secure
- http://docs.aws.amazon.com/workdocs/latest/adminguide/cloudtrail_logging.html

ファイル名やディレクトリ名には、PHI を含めないでください。

Amazon Inspector

Amazon Inspector は、自動化されたセキュリティ評価サービスであり、AWS にデプロイされたアプリケーションのセキュリティとコンプライアンスを向上させることを目的としています。Amazon Inspector は、自動でアプリケーションを評価し、脆弱性やベストプラクティスからの逸脱がないかどうかを確認します。評価後、セキュリティの検出結果を重大性の順に示した詳細なリストが作成されます。

Amazon Inspector は、PHI を格納する EC2 インスタンスで実行できます。Amazon Inspector ではネットワークを介して送信されるすべてのデータと、保管されるすべてのテレメトリデータが暗号化されます。

Amazon Kinesis Streams

Amazon Kinesis Data Streams を使用すると、特定のニーズに合わせてストリーミングデータを処理、分析するカスタムアプリケーションを構築できます。サーバー側の暗号化機能を使用すると、保存データを暗号化できます。サーバー側の暗号化が有効になっている場合、データがディスクに保管される前に、AWS Key Management Service (AWS KMS) のキーを使用してデータが暗号化されます。詳しくは、http://docs.aws.amazon.com/streams/latest/dev/server-side-encryption.html をご覧ください。

PHI を格納する Amazon S3 への接続には、暗号化された転送 (HTTPS など) を受け入れるエンドポイントが使用されていなければなりません。リージョンごとのエンドポイントのリストについては、http://docs.aws.amazon.com/general/latest/gr/rande.html#ak_region をご覧ください。

AWS Lambda

AWS Lambda を使用すれば、サーバーをプロビジョニングしたり管理したりしなくても、コードを実行できるようになります。AWS Lamba では、各リージョンの複数のアベイラビリティーゾーンにまたがって Amazon Elastic Compute Cloud (Amazon EC2) のインスタンスフリートを使用することで、AWS インフラストラクチャに優れた可用性、セキュリティ、パフォーマンス、スケーラビリティをもたらします。

AWS Lambda の使用時に PHI が暗号化された状態を維持するためには、外部リソースへの接続で、HTTPS や SSL/TLS などの暗号化プロトコルを使用しなければなりません。例えば、Lambda プロシージャから S3 にアクセスする場合、アドレスを https://bucket.s3-aws-region.amazonaws.com に指定してアクセスする必要があります。実行中のプロシージャ内で PHI を保管したりアイドル状態にしたりする場合は、AWS KMS または AWS CloudHSM から取得したキーを使用して、クライアント側あるいはサーバー側でデータを暗号化してください。AWS Lambda サービスで Lambda 関数をトリガーする際は、AWS API Gateway に関するガイダンスに従う必要があります。他の AWS サービスのイベントを使用して AWS Lambda 関数をトリガーする場合、イベントデータに PHI が含まれていたり、PHI 自体がイベントであったりしてはなりません。例えば、S3 でのオブジェクト受信などといった S3 イベントによって Lambda プロシージャをトリガーする場合、Lambda に渡されるオブジェクト名には PHI が含まれないようにしてください。ただし、オブジェクト自体に PHI を含めることはできます。

AWS Batch

AWS Batch を使用することにより、開発者、科学者、およびエンジニアは、数十万件のバッチコンピューティングジョブを AWS で簡単かつ効率的に実行できます。AWS Batch では、送信されたバッチジョブのボリュームと特定のリソース要件に応じて、コンピューティングリソース (CPU やメモリ最適化インスタンス) の最適な数量とタイプを動的にプロビジョニングします。AWS Batch は、AWS のコンピューティングサービスと機能を最大限に活用して、バッチコンピューティングワークロードを計画、スケジュール、実行します。

AWS ECS を対象としたガイダンスと同様、PHI を AWS Batch のジョブ定義、ジョブキュー、またはタグに直接含めないでください。AWS Batch でスケジュールされて実行されるジョブで、暗号化された PHI を操作することはできます。ジョブのステージから AWS Batch に返される情報にも、PHI を含めな

いでください。AWS Batch で実行されるジョブで PHI を送信または受信する必要がある場合は必ず、その接続を HTTPS または SSL/TLS で暗号化する必要があります。

Amazon Connect

Amazon Connect は、動的でパーソナライズされた自然なカスタマーエンゲージメントをあらゆる規模で実現できる、セルフサービス型のクラウドベースのコンタクトセンターです。

Amazon Connect 内のユーザー、セキュリティプロファイル、およびコンタクトフローに関連するフィールドには、PHI を含めないでください。

Amazon Route 53

Amazon Route 53 は、ドメイン名の登録、インターネットトラフィックドメインリソースのルーティング、そしてこれらのリソースの正常性チェックに対応する機能を備えた、マネージド型 DNS サービスです。Amazon Route 53 は HIPAA 対応サービスですが、PHI が含まれるデータの暗号化はサポートしていないため、Amazon Route 53 内のリソース名やタグに PHI を保管することはできません。PHI を転送または保管するドメインリソース (例えば、Amazon EC2 で実行されるウェブサーバーや、Amazon S3 などのストレージ) にアクセスするために、Amazon Route 53 を使用することはできます。

AWS CloudHSM

AWS CloudHSM は、AWS クラウドでの暗号化キーの生成と使用を容易にする、クラウドベースのハードウェアセキュリティモジュール (HSM) です。CloudHSM では、FIPS 140-2 のレベル 3 認証済みの HSM を使用して、暗号化キーを管理できます。さらに、PKCS#11、Java Cryptography Extensions (JCE)、Microsoft CryptoNG (CNG) ライブラリといった業界標準の API を使用して、アプリケーションを柔軟に統合することができます。また、CloudHSM は規格に準拠しているため、他のほとんどの商用 HSM にお客様のすべてのキーをエクスポートできます。

Cloud HSM は、ハードウェアアプライアンスのキー管理サービスであるため、PHI を保管したり転送したりすることはできません。このサービスに固有のガイダンスは、タグ (メタデータ) に PHI を保管しないようにすることだけです。

Amazon ElastiCache for Redis

Amazon ElastiCache for Redis は、データストアまたはキャッシュとして使用できる、Redis 対応のインメモリデータ構造サービスです。

Amazon ElastiCache for Redis で PHI を保管するには、最新バージョンのコンプライアンス対応 ElastiCache for Redis エンジンを実行する必要があります。Amazon ElastiCache for Redis では、以下のインスタンスタイプおよび Redis エンジンのバージョンで、PHI の保管をサポートします。

- インスタンスタイプ t2、m3、m4、r3
- ElastiCache for Redis エンジンのバージョン 3.2.6

ElastiCache エンジンの選択について詳しくは、http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/SelectEngine.Uses.html をご覧ください。

保存データを暗号化するようにクラスターとクラスター内のノードを設定し、転送時の暗号化および Redis コマンドの認証を有効にする必要もあります。以下で詳しく説明します。

保管時の暗号化

Amazon ElastiCache for Redis では、保存データを保護するために、クラスターに対してデータ暗号化を有効にできるようになっています。クラスターの作成時に保管時のデータ暗号化を有効にすると、ディスク上のデータと自動 Redis バックアップに含まれるデータが暗号化されます。ディスク上のデータの暗号化には、ハードウェアアクセラレーション対応の高度な暗号化規格 (AES) による 512 ビットの対称キーが使用されます。一方、Redis バックアップの暗号化には、Amazon S3 で管理される暗号化キー (SSE-S3) が使用されます。サーバー側の暗号化が有効になっている S3 バケットでは、データを保存する前に、ハードウェアアクセラレーション対応の高度な暗号化規格 (AES) による 256 ビットの対称キーを使用してデータが暗号化されます。Amazon S3 で管理された暗号化キー (SSE-S3) について詳しくは、http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html をご覧ください。暗号化を有効にして稼働している (単一または複数のノードからなる) ElastiCache Redis クラスターでは、本ホワイトペーパーの公開時点で効力のあるガイダンスに従って、保存データが暗号化されます。この

暗号化では、ディスク上のデータと、S3 バケット内の自動バックアップに含まれるデータの両方が対象になります。このガイダンスは更新される可能性があるため、Amazon ElastiCache for Redis の暗号化を継続的に評価して、お客様のコンプライアンス要件と規制上の要件を満たしているかどうかを判断してください。Amazon ElastiCache for Redis を使用した保管時のデータ暗号化について詳しくは、http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/at-rest-encryption.html をご覧ください。

転送時の暗号化

Amazon ElastiCache for Redis では、転送時のデータ暗号化に TLS を使用します。PHI を格納する ElastiCache for Redis への接続には、転送時の暗号化が使用されていなければなりません。設定を評価して、ガイダンスに従っていることを確認してください。詳しくは、http://docs.aws.amazon.com/AmazonElastiCache/latest/APIReference/API_CreateReplicationGroup.html をご覧ください。転送時の暗号化を有効にする方法については、http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/in-transit-encryption.html をご覧ください。

認証

PHI を格納する (単一/複数のノードからなる) Amazon ElastiCache for Redis クラスターには、Redis コマンドの認証を有効にするための Redis AUTH トークンが必要です。Redis AUTH は、保管時の暗号化と転送時の暗号化の両方が有効にされている場合に利用できます。Redis AUTH には、以下の制約事項に従った強力なトークンを使用してください。

- 印刷可能な ASCII 文字だけが含まれていること
- 16 文字以上、128 文字以下の長さであること
- 特殊文字 /、"、@ が含まれていないこと

このトークンは、(単一/複数のノードからなる) Redis レプリケーショングループの作成時に、リクエストパラメータ内に設定する必要がありますが、後で新しい値で更新することもできます。このトークンは、AWS Key Management Service (KMS) を使用して暗号化されます。Redis AUTH について詳しくは、

http://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/auth.html をご覧ください。

Amazon CloudWatch

Amazon CloudWatch Logs を使用すると、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、AWS CloudTrail、Amazon Route 53、およびその他のソースのログファイルを監視、保管したり、ログファイルにアクセスしたりできます。さらに、CloudWatch Logs から関連するログデータを取得することもできます。ログデータは転送時および保管時に暗号化されるため、他のサービスから送信されて CloudWatch Logs に配信された PHI を再び暗号化する必要はありません。

Amazon EC2 Container Registry

Amazon EC2 Container Registry (ECR) には Amazon EC2 Container Service (ECS) が統合されいるため、Amazon ECS で実行するアプリケーションのコンテナイメージを簡単に保管、実行、管理できます。タスク定義で Amazon ECR リポジトリを指定すると、アプリケーションに適したイメージがそのリポジトリから取得されます。

PHI が含まれるコンテナイメージで Amazon ECR を使用するために特に必要となる手順はありません。コンテナイメージは、転送時および保管時に、Amazon S3 のサーバー側の暗号化 (SSE-S3) を使用して暗号化されます。

Amazon Macie

Amazon Macie は、機械学習によって AWS 内の機密データを自動的に検出、分類、保護するセキュリティサービスです。PHI や知的財産などの機密データが見つかると、それらのデータのアクセス状況や移動状況を確認できるよう、ダッシュボードやアラートが表示されます。この完全マネージド型サービスでは、データアクセスアクティビティに異常がないか継続的に監視され、不正アクセスや不注意によるデータ漏洩のリスクが検出された場合には詳細なアラートが生成されます。

Amazon Macie は、Amazon S3 に保管されているオブジェクトだけに作用します。Amazon Macie を構成するためだけに、PHI を入力したり保管したりする必要はありません。Amazon Macie の監視対象となっている S3 バケットに保管するすべてのオブジェクトは、保管時に暗号化する必要があります。ただし、

Amazon Macie では、クライアント側の暗号化を使用して暗号化されたオブジェクトを読み取って分類することはできません。S3 上のオブジェクトに保管された PHI の監視を効果的に行うには、サーバー側の暗号化 (SSE-S3) または KMS で管理されたキー (SSE-KMS) を使用してください。

Amazon QuickSight

Amazon QuickSight は、データの可視化、アドホック分析を可能にするビジネス分析サービスです。このサービスを利用することで、お客様は所有データからビジネス上の洞察を素早く得ることができます。AWS データソースの検出がサポートされ、組織が数十万人のユーザーに拡張することを可能にします。堅牢なインメモリエンジン (SPICE) を使用することで優れた応答性を実現します。

Amazon QuickSight で PHI が含まれるデータを処理する場合は、SPICE に保管されるデータの保管時暗号化をサポートする Enterprise Edition のみを使用できます。データ暗号化は、AWS で管理されるキーを使用して行われます。

AWS マネージドサービス

AWS マネージドサービスは、AWS のインフラストラクチャを継続的に管理するサービスです。ベストプラクティスを実装した AWS マネージドサービスでインフラストラクチャを管理することにより、運用上のオーバーヘッドとリスクを低減できます。AWS マネージドサービスを使用することで、変更リクエスト、監視、パッチ管理、セキュリティ、バックアップサービスなどの一般的なアクティビティが自動化されます。さらに、インフラストラクチャをプロビジョニング、実行、サポートするための、ライフサイクル全体にわたるサービスも用意されています。

PHI が含まれるデータを処理する AWS ワークロードは、AWS マネージドサービスを使用して管理することができます。AWS マネージドサービスを使用するとしても、PHI に使用できる AWS サービスが左右されることはありません。AWS マネージドサービスで提供されるツールと自動化は、PHI の保管や転送には使用できません。

AWS Fargate

AWS Fargate は、サーバーやクラスターの管理の必要なしにコンテナを実行できるようにするためのテクノロジーです。AWS Fargate を使用すれば、コンテナを実行するために仮想マシンのクラスターをプロビジョニング、設定、スケーリングする必要がなくなります。したがって、サーバータイプを選択したり、クラスターをスケーリングするタイミングを決定したり、クラスターのパッキングを最適化したりする必要もなくなります。AWS Fargate により、サーバーやクラスターの操作や検討が不要になり、アプリケーションを実行するインフラストラクチャの管理ではなく、アプリケーションの設計や構築に注力できるようになります。

PHI を処理するワークロードと Fargate を連動させるために必要な設定はありません。Fargate でコンテナーワークロードを実行するには、Amazon ECS などのコンテナーオーケストレーションサービスを使用します。Fargate が管理するのは基盤となるインフラストラクチャのみであり、オーケストレーション対象のワークロードに含まれるデータを使用したり処理したりすることはありません。Fargate によって起動されたコンテナーで PHI にアクセスする場合も、HIPAA の要件に従って、PHI を転送時や保管時に暗号化する必要があります。本書で説明する AWS ストレージオプションのそれぞれで、保管時の暗号化に各種のメカニズムを使用できます。

監査、バックアップ、障害復旧

HIPAA のセキュリティルールでは、徹底した監査機能、データバックアップ手順、障害復旧メカニズムも要件とされています。AWS のサービスには、これらの要件に対処するのに役立つ多数の機能が含まれています。

HIPAA と HITECH の要件に準拠した情報システムを設計する際は、監査機能を導入する必要があります。監査機能により、セキュリティアナリストが詳細なアクティビティログやレポートを調べて、ユーザーアクセス、IP アドレスエントリー、アクセスされたデータを確認できるようにします。監査に備えて、これらのデータを追跡し、ログに記録し、中央の場所に長期間保管する必要があります。Amazon EC2 を使用すれば、仮想サーバーでも従来のハードウェアの場合と同じように、パケット層まで掘り込んだアクティビティのログファイルと監査を実行できます。さらに、仮想サーバーインスタンスに到達したすべての IP トラフィックを追跡することもできます。管理者は長期にわたり信頼

できるストレージとして、Amazon S3 にこれらのログファイルをバックアップできます。

HIPAA が適用される事業体は、緊急時にデータを保護するための危機管理計画を策定し、電子的な PHI の正確なコピーを作成して取得可能な状態に維持する必要があります。AWS にデータバックアップ計画を実装できるよう、Amazon EBS では Amazon EC2 仮想サーバーインスタンスの永続ストレージを使用できます。永続ストレージのボリュームは、標準のブロックデバイスとして公開して、インスタンスの寿命とは関係なく存続可能な外部ストレージとすることができます。HIPAA のガイドラインに従って、Amazon EBS ボリュームのポイントインタイムスナップショットを作成することもできます。作成されたスナップショットは自動的に Amazon S3 に保管されて、複数のアベイラビリティーゾーンに複製されます。これらのアベイラビリティーゾーンはそれぞれに異なるロケーションにあり、互いの障害から隔離されるように設計されています。したがって、複製されたスナップショットにいつでもアクセス可能で、データを保護して長期耐久性を実現できます。Amazon S3 では、データストレージおよび自動バックアップの高可用性ソリューションも提供しています。このソリューションでは、ファイルやイメージを Amazon S3 にロードするだけで、自動的に複数の冗長コピーが作成されて、複数の異なるデータセンターに保管されます。これらのファイルは、いつでも、(アクセス権に基づき) どこからでもアクセス可能で、意図的に削除されるまで保管されます。

障害復旧とは、災害発生時に組織のデータと IT インフラストラクチャを保護するプロセスのことです。障害復旧は一般に、準拠するのに最も費用がかかる HIPAA 要件の 1 つです。障害復旧の要件を満たすには、高可用性を備えたシステムを維持し、データとシステムの両方を別の場所に複製し、この両方に常にアクセスできる状態にしなければなりません。AWS では、各種の障害復旧メカニズムが本質的に備わっています。

Amazon EC2 を使用すると、管理者は極めて短時間でサーバーインスタンスを起動し、Elastic IP アドレス (クラウドコンピューティング環境での静的 IP アドレス) を使用してマシン間のグレースフルフェイルオーバーに対応できます。また、Amazon EC2 にもアベイラビリティーゾーンが用意されているため、管理者は複数のアベイラビリティーゾーンで Amazon EC2 インスタンスを起動することで、地理的に分散された、耐障害性を備えたシステムを構築できます。このようなシステムであれば、ネットワーク障害、自然災害、さらにダウンタイムの原因となる他のほとんどの問題が発生したとしても、極めて優れた回復力を発揮します。また、Amazon S3 を使用すると、複製されたデータが自動的に異なる複数のデータセンターに保管されます。これによって、99.99%

の可用性を達成するよう設計された、信頼性の高いデータストレージを使用できるようになります。

障害復旧について詳しくは、http://aws.amazon.com/disaster-recovery/ に掲載されている AWS ホワイトペーパー「災害対策」をご覧ください。

文書改訂

日付	説明
2018 年 6 月	日本語版発行
2018 年 1 月	「AWS Fargate」のセクションを追加。
2017 年 11 月	「Amazon EC2 Container Registry」、「Amazon Macie」、「Amazon QuickSight」、「AWS マネージドサービス」の各セクションを追加。
2017 年 11 月	「Amazon ElastiCache for Redis」および「Amazon CloudWatch」のセクションを追加。
2017 年 10 月	「Amazon SNS」、「Amazon Route53」、「AWS Storage Gateway」、「AWS Snowmobile」、「AWS CloudHSM」の各セクションを追加、AWS Key
2017 年 9 月	「Amazon Connect」、「Amazon Kinesis Streams」、「Amazon RDS (Maria) DB」、「Amazon RDS SQL Server」、「AWS Batch」、「AWS Lambda」、
2017 年 8 月	「Amazon EC2 Systems Manager」および「Amazon Inspector」のセクションを追加。
2017 年 7 月	「Amazon WorkSpaces」、「Amazon WorkDocs」、「AWS Directory Service」、「Amazon ECS」の各セクションを追加。
2017 年 6 月	「Amazon CloudFront」、「AWS WAF」、「AWS Shield」、「Amazon S3 Transfer Acceleration」の各セクションを追加。
2017 年 5 月	EC2 および EMR で PHI を処理する専用インスタンスまたは専用ホストに関する要件を削除。
2017 年 3 月	「コンプライアンスプログラムによる AWS 対象範囲内のサービス」ページを参照するようにサービス一覧を更新。Amazon API Gateway の説明を追加。
2017 年 1 月	最新のテンプレートに更新。
2016 年 10 月	初版