付録. 第4章 システム・運用要件回答（詳細）

第1節　基本サービス要件

<table>
<tr><th>項目</th><th>要件</th><th>回答</th></tr>
<tr><td>1-1
提供プラットフォーム種別</td><td>仮想サーバー共通の提供スペック(CPU/メモリ/ディスク)</td><td>EC2(仮想サーバー)ならびにRDS(データベース)では、数多くのインスタンスタイプが提供されている。東京リージョンにて選択可能なインスタンスタイプは、以下の通りである。

EC2
<table>
<tr><th>インスタンスタイプ</th><th>vCPU</th><th>ECU</th><th>メモリ(GiB)</th><th>インスタンスストレージ(GB)</th></tr>
<tr><td colspan="5">T2 一般的な目的 - 現行世代　バーストパフォーマンスインスタンス※7</td></tr>
<tr><td>t2.micro</td><td>1</td><td>可変</td><td>1</td><td>EBS のみ</td></tr>
<tr><td>t2.small</td><td>1</td><td>可変</td><td>2</td><td>EBS のみ</td></tr>
<tr><td>t2.medium</td><td>2</td><td>可変</td><td>4</td><td>EBS のみ</td></tr>
<tr><td colspan="5">M3 一般的な目的 - 現行世代　※3</td></tr>
<tr><td>m3.medium</td><td>1</td><td>3</td><td>3.75</td><td>1 x 4 SSD</td></tr>
<tr><td>m3.large</td><td>2</td><td>6.5</td><td>7.5</td><td>1 x 32 SSD</td></tr>
<tr><td>m3.xlarge</td><td>4</td><td>13</td><td>15</td><td>2 x 40 SSD</td></tr>
<tr><td>m3.2xlarge</td><td>8</td><td>26</td><td>30</td><td>2 x 80 SSD</td></tr>
<tr><td colspan="5">C3 コンピューティング最適化 - 現行世代</td></tr>
<tr><td>c3.large</td><td>2</td><td>7</td><td>3.75</td><td>2 x 16 SSD</td></tr>
<tr><td>c3.xlarge</td><td>4</td><td>14</td><td>7.5</td><td>2 x 40 SSD</td></tr>
<tr><td>c3.2xlarge</td><td>8</td><td>28</td><td>15</td><td>2 x 80 SSD</td></tr>
<tr><td>c3.4xlarge</td><td>16</td><td>55</td><td>30</td><td>2 x 160 SSD</td></tr>
<tr><td>c3.8xlarge</td><td>32</td><td>108</td><td>60</td><td>2 x 320 SSD</td></tr>
<tr><td colspan="5">G2 GPU インスタンス - 現行世代</td></tr>
<tr><td>g2.2xlarge</td><td>8</td><td>26</td><td>15</td><td>60 SSD</td></tr>
<tr><td colspan="5">R3 メモリの最適化 - 現行世代</td></tr>
<tr><td>r3.large</td><td>2</td><td>6.5</td><td>15</td><td>1 x 32 SSD</td></tr>
<tr><td>r3.xlarge</td><td>4</td><td>13</td><td>30.5</td><td>1 x 80 SSD</td></tr>
<tr><td>r3.2xlarge</td><td>8</td><td>26</td><td>61</td><td>1 x 160 SSD</td></tr>
<tr><td>r3.4xlarge</td><td>16</td><td>52</td><td>122</td><td>1 x 320 SSD</td></tr>
<tr><td>r3.8xlarge</td><td>32</td><td>104</td><td>244</td><td>2 x 320 SSD</td></tr>
<tr><td colspan="5">I2 ストレージの最適化 - 現行世代</td></tr>
<tr><td>i2.xlarge</td><td>4</td><td>14</td><td>30.5</td><td>1 x 800 SSD</td></tr>
<tr><td>i2.2xlarge</td><td>8</td><td>27</td><td>61</td><td>2 x 800 SSD</td></tr>
<tr><td>i2.4xlarge</td><td>16</td><td>53</td><td>122</td><td>4 x 800 SSD</td></tr>
<tr><td>i2.8xlarge</td><td>32</td><td>104</td><td>244</td><td>8 x 800 SSD</td></tr>
<tr><td>hs1.8xlarge</td><td>16</td><td>35</td><td>117</td><td>24 x 2048</td></tr>
</table>

RDB
<table>
<tr><th>インスタンスタイプ</th><th>vCPU</th><th>メモリ(GiB)</th><th>PIOPS 用に最適化</th><th>ネットワークパフォーマンス</th></tr>
<tr><td colspan="5">M3 スタンダード - 現行世代</td></tr>
<tr><td>db.m3.medium</td><td>1</td><td>3.75</td><td>-</td><td>中</td></tr>
<tr><td>db.m3.large</td><td>2</td><td>7.5</td><td>-</td><td>中</td></tr>
<tr><td>db.m3.xlarge</td><td>4</td><td>15</td><td>はい</td><td>中</td></tr>
<tr><td>db.m3.2xlarge</td><td>8</td><td>30</td><td>はい</td><td>高</td></tr>
<tr><td colspan="5">R3 メモリの最適化 - 現行世代</td></tr>
<tr><td>db.r3.large</td><td>2</td><td>15</td><td>-</td><td>中</td></tr>
<tr><td>db.r3.xlarge</td><td>4</td><td>30.5</td><td>はい</td><td>中</td></tr>
<tr><td>db.r3.2xlarge</td><td>8</td><td>61</td><td>はい</td><td>高</td></tr>
<tr><td>db.r3.4xlarge</td><td>16</td><td>122</td><td>はい</td><td>高</td></tr>
<tr><td>db.r3.8xlarge</td><td>32</td><td>244</td><td>-</td><td>10 ギガビット</td></tr>
<tr><td colspan="5">T1 マイクロインスタンス</td></tr>
<tr><td>db.t1.micro</td><td>1</td><td>0.613</td><td>--</td><td>非常に低</td></tr>
<tr><td colspan="5">M1 モールインスタンス</td></tr>
<tr><td>db.m1.small</td><td>1</td><td>1.7</td><td>-</td><td>低</td></tr>
</table>

※1. 各インスタンスタイプの右括弧内は、左からvCPU*仮想コア数/メモリ/インスタンスストレージの各スペックとなる。
※2. ECU: 1つの1.0-1.2GHz 2007 Opteronまたは2007 Xeonプロセッサ(1.7GHz相当)のCPU 能力に等しい能力を有している。
※3. EBS最適化オプションが選択可能で、このオプションを選択すると、EC2とEBS間のスループットについて、選択したインスタンスタイプに応じて、500Mbpsまたは1,000Mbpsを確保することが可能となる。
※4. 10GbEのクラスターネットワークをサポートしている。
※5. ゲストOSの種別次第で、ご利用可能なインスタンスタイプが異なる。
※6. EC2/RDSの各インスタンスタイプについては、今後も種別が増えていく傾向が続くと予想される。
※7. T2 インスタンスは、ベースラインを超えてバーストする能力がある。

【参考 URL】
[EC2] http://aws.amazon.com/jp/ec2/pricing/
[RDS] http://aws.amazon.com/jp/rds/pricing/</td></tr>
<tr><td></td><td>ゲストOS</td><td>EC2では、Linux/Windows系の数多くのゲストOSが利用可能で、東京リージョンにて選択可能な主なゲストOSは、以下の通りである。(※全てOSライセンスも含めて提供される)

▼Linux系
・Amazon Linux (32/64bit)
・Amazon Linux(HVM) (64bit)
・Red Hat Enterprise Linux(RHEL) 5/6 (32/64bit)
・Red Hat Enterprise Linux(RHEL) 6 (HVM) (64bit)
・Red Hat Enterprise Linux(RHEL) 7 (HVM) (64bit)
・Red Hat Enterprise Linux 6 for Cluster Instances (64bit)
・SUSE Linux Enterprise Server 11 (32/64bit)
・Cluster Instances HVM SUSE Linux Enterprise 11 (64bit)
・Ubuntu Server 10/11/12/13 (32/64bit)
・CentOS 6 (32/64bit)
・Debian GNU/Linux (32/64bit)</td></tr>
</table>

		▼Windows系 ・Microsoft Windows Server 2003 R2 および SQL Server Standard 2005 ・Microsoft Windows Server 2003 R2 および SQL Server Express 2005 & IIS ・Microsoft Windows Server 2003 R2 Base (32 ビット / 64 ビット) ・Microsoft Windows Server 2008 Base (32 ビット / 64 ビット) ・Microsoft Windows Server 2008 および SQL Server Standard 2008 ・Microsoft Windows Server 2008 および SQL Server Express 2008 & IIS ・Microsoft Windows Server 2008 R2 Base ・Microsoft Windows Server 2008 R2 クラスター用 ・Microsoft Windows Server 2008 R2 および SQL Server Standard 2012 ・Microsoft Windows Server 2008 R2 および SQL Server Standard 2008 ・Microsoft Windows Server 2008 R2 および SQL Server Express 2012 & IIS ・Microsoft Windows Server 2008 R2 および SQL Server Express 2008 & IIS ・Microsoft Windows Server 2012 RTM ・Microsoft Windows Server 2012 RTM および SQL Server Web / Express / Standard 2014 ・Microsoft Windows Server 2012 RTM および SQL Server Express / Standard 2012 ・Microsoft Windows Server 2012 R2 ・Microsoft Windows Server 2012 R2 および SQL Server Web / Express / Standard 2014 【参考 URL】 http://aws.amazon.com/jp/windows/amis/ ※ ゲストOSの種別次第で、ご利用可能なインスタンスタイプが異なる。 また、各ゲストOS毎に選択可能な言語およびタイムゾーンの設定が可能である。
	データベースエンジン	東京リージョンにて選択可能なRDSのデータベースエンジンは、以下の通りである。 ・MySQL Community Edition ・PostgreSQL ・Oracle Database Standard Edition One/Standard Edition/Enterprise Edition ・Microsoft SQL Server Express/Web/Standard/Enterprise Edition 【参考 URL】 http://aws.amazon.com/jp/rds/
	仮想サーバー/データベースサーバーの契約体系	EC2/RDSでは、以下の2種類の契約体系が用意されており、用途・ご利用期間・ご予算等に条件に応じて、使い分けが可能である。 (1) オンデマンドインスタンス ・契約期間/初期費用ともに無し ・使用時間単位の従量課金 (2) リザーブドインスタンス ・1年もしくは3年契約 ・事前に予約金を支払う事で、使用時間単位の従量課金の割引が可能 ・使用頻度に応じて3種類のタイプ(軽度/中度/重度使用)が有る 更にEC2では、スポットインスタンスでのご契約も可能である。 (3) スポットインスタンス ・入札方式(入札価格が上回る限りはインスタンスを使用可能) ・需要と供給に基づいて時価(スポット価格)が適宜変動 ※EC2/RDSの各インスタンスの料金については、適宜価格改定がなされており、今後もその傾向が続くと予想される。 【参考 URL】 [EC2] http://aws.amazon.com/jp/ec2/pricing/ [RDS] http://aws.amazon.com/jp/rds/pricing/
	ストレージサービス	AWSでは、主に以下の4種類のストレージが用意・提供されており、用途やご予算等に応じて、使い分けが可能である。各々のストレージの主な特徴は以下の通りである。 **(1) インスタンスストア** ・EC2とセットで提供されるストレージ ・インスタンスが稼動している間のみデータを保持 （※インスタンスを削除すると、インスタンスストアに格納されたデータも削除） ・ユースケース: Linux系サーバのSwap領域など一時的なデータ保管領域 **(2) EBS** ・平均的なパフォーマンスが約100 IOPSのハードディスクをベースとした「Magnetic volumes」と、最大4,000 IOPSがサポートされており、IOPS単位で課金可能なSSDベースの「provisioned IOPS volumes」、1GBあたり3 IOPSを保証し、最大3,000 IOPSまでバースト可能なSSDベースの「General Purpose volumes」の3種類から選択可能 ・1つのEBSボリュームサイズは最大1TB(1,024GB)まで ・実際の使用量に関わらず、予約・確保した容量分の課金が発生 ・General Purpose volumesのバースト可能な時間は、I/O Creditの残高とベースパフォーマンスに依存 ・EBSはAES-256で暗号化が可能。 （※ブートボリュームの暗号化は未サポート、作成済の非暗号化EBSスナップショットから暗号化EBSは作成不可） ・ユースケース: Linux系/Windows系のシステム領域およびデータ領域 【参考 URL】 http://aws.amazon.com/jp/ebs/ **(3) S3** ・容量無制限 ・最大5TBまでのデータを含むオブジェクトの書き込み・読み込み・削除が可能 ・サーバーサイド暗号化(SSE)が使用可能 ・実際の使用量分だけ課金 ・ユースケース: オンプレミス環境/AWS環境のシステムバックアップ/データバックアップ領域 （EBSスナップショットや仮想サーバーのイメージファイル(AMI)のデータ格納領域もS3になる。） 【参考 URL】 http://aws.amazon.com/jp/s3/ **(4) Glacier** ・データアーカイブ用途のストレージ(従来のテープバックアップの代替) ・データリストアまでに一般的に3～5時間必要 ・実際の使用量分だけ課金 ・ユースケース: ログデータ等のアーカイブデータ格納領域 【参考 URL】 http://aws.amazon.com/jp/glacier/

1-2 リソース準備までの時間	新規アカウント作成までの時間	AWSで新規アカウントを作成する際は、以下の5つの手順で登録を進めることになる。 所要時間は、おおむね5～10分で登録完了する。 (1) サインインとAWSアカウント作成 (2) ログイン情報設定 (3) お問い合わせ情報入力 (4) お支払情報入力 (5) 自動音声（電話による身元確認） 【参考 URL】 http://aws.amazon.com/jp/register-flow/
	リソース準備までの時間	AWSは、オンデマンド性/拡張性に優れたサービスで、AWS Management CosoleおよびAWSコマンドラインツール(API連携)経由で、柔軟になおかつスピーディに、システムリソースの伸縮が可能である。 【特記事項】 ・AWSの場合、課金は最短で1時間単位となっている。 ・AWSのサービス仕様上、リソースの拡張・追加に関して、一定の上限が設定されている。 【参考 URL】 http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html ・ただし、上限緩和申請を提示することで、上限を変更することが可能で、申請後、概ね3～5営業日程度で上限変更が可能である。 ・EC2/RDSインスタンスのリソースの確保が必須である場合は、リザーブドインスタンスを選択する必要がある。 ・vCPUや仮想コア数、メモリ容量を変更されたい場合は、インスタンスタイプを変更する必要がある。インスタンスの変更に際しては、仮想サーバーの停止と起動が必要となる。
1-3 管理ポータル機能	機能概要	AWSでは、「Management Console」という管理ポータル機能が用意されている。 **▼「Management Console」の主な特徴** ・Webブラウザで閲覧・設定することが可能。 ・IAM(Identity and Access Management)にてユーザー・グループ毎にロールや権限(FullAccess/PowerUser/Read Only)を組み合わせて設定することが可能。 ・1つのAWSアカウントで、標準で5,000ユーザー/100グループまで作成可能。(※上限緩和申請を提出することで上限変更も可能) ・パスワードポリシー(パスワードの最低文字数指定、大文字/小文字/数字/非英数字のパスワード設定、ユーザー自身でのパスワード変更許可)を個別に設定することが可能。 ・よりセキュアに管理ポータル機能をお使いになりたい場合は、ハードウエアデバイスもしくはソフトウエアベースのMFA(Multi-Factor Authentication：多要素認証)を組み合わせて、ワンタイムパスワードによる認証を実装することも可能。 【参考 URL】 [Management Console] http://aws.amazon.com/jp/console/ [IAM] http://aws.amazon.com/jp/iam/
	制御・確認が可能な機能	「Management Console」にて、制御・確認が可能なサービスは、以下の通りである。 **▼「Management Console」で制御・確認可能なサービス** [コンピューティング & ネットワーキング] Amazon EC2/Auto Scaling/Elastic Load Balancing/Amazon WorkSpaces/Amazon VPC/Amazon Route 53/AWS Direct Connect [ストレージとコンテンツ配信] Amazon S3/Amazon Glacier/Amazon EBS/AWS Import/Export/AWS Storage Gateway/Amazon CloudFront [データベース] Amazon RDS/Amazon DynamoDB/Amazon ElastiCache/Amazon Redshift/Amazon SimpleDB [分析] Amazon EMR/Amazon Kinesis/AWS Data Pipeline [デプロイ＆マネジメント] AWS Identity & Access Management/AWS CloudTrail/Amazon CloudWatch/AWS Elastic Beanstalk/AWS CloudFormation/AWS OpsWorks/AWS CloudHSM [アプリケーションサービス] Amazon AppStream/Amazon CloudSearch/Amazon SWF/Amazon SQS/Amazon SES/Amazon SNS/Amazon Elastic Transcoder ※Management Console経由で制御・可能なサービスは、今後も増えていくことが予想される。 【参考 URL】 http://aws.amazon.com/jp/console/
	仮想サーバーに関する統計情報	「Management Console」にて、標準で閲覧可能な仮想サーバーに関する統計情報は、以下の通りである。 **▼「Management Console」にて標準で閲覧可能な統計情報 (EC2)** ・CPU Utilization (%) ・CPU Credit Usage/Balance(Count) ・Disk Reads/Writes (Bytes) ・Disk Read/Write Operations (Operations) ・Network In/Out (Bytes) ・Status Check Failed(Any/Instance/System) (Count) **▼「Management Console」にて標準で閲覧可能な統計情報 (EBS)** ・Read/Write Bandwidth (KiB/s) ・Read/Write Throughput (Ops/s) ・Average Queue Length (Operations) ・Time Spent Idle (%) ・Average Read/Write Size (KiB/op) ・Average Read/Write Latency (ms/op) ・Throughput Percentage (%) ・Consumed Read Write Operations (count)

	その他統計情報	「Management Console」にて、標準で閲覧可能なその他サービスに関する統計情報は、以下の通りである。 **▼「Management Console」にて標準で閲覧可能な統計情報 (ELB)** ・Sum HTTP 2XXs/4XXs/5XXs (Count) ・Sum ELB HTTP 4XXs/5XXs (Count) ・Helthy/Unhelthy Hosts (Count) ・Average Latency (Seconds) ・Sum Requests (Count) ・Backend Connection Errors (Count) ・Surge Queue Length (Count) ・Spillover Count (Count) **▼「Management Console」にて標準で閲覧可能な統計情報 (RDS)** ・CPU Utilication (%) ・DB Connections (Count) ・Free Strage Space (MB) ・Freeable Memory (MB) ・Write/Read IOPS (Count/Second) ・Queue Depth (Count) ・Replica Lag (Seconds) ・Binary Log Disk Usage (MB) ・Write/Read Throughput (MB/Second) ・Swap Usage (MB) ・Read/Write Latency (Seconds) ・Network Receive/Transmit Throughput (MB/Second) ・CPU Credit Usage/Balance(Count)
	API連携	AWSでは、数多くのプログラミング言語またはプラットフォーム用のSDKが用意されており、Management Consoleを経由せずに、コマンドラインでも各種AWSサービスが操作可能となっている。 **▼AWS SDK** Java/.Net/Node.js/Python/PHP/Ruby/ Android/iOSといったプログラミング言語またはプラットフォーム用に調整されたAPIを使用して、AWSサービスをプログラム操作することができるSDKが提供されている。なお、プログラム操作時の通信は、原則的にhttpsプロトコルとなる。
1-5 災害対策	日本国内での災害対策(クラウドサービスのみを利用する場合)	東京リージョンでは、物理的に40～60km離れた2つのアベイラビリティゾーンにてサービス提供基盤が配置されている。 **▼仮想サーバー** 複数のアベイラビリティゾーンに跨いでEC2(仮想サーバー)を配置し、ELBにて負荷分散させることで単一アベイラビリティゾーンで障害が発生したとしても、システムを継続稼働させることが可能である。 ※アベイラビリティゾーン間を跨ぐトラフィックには、別途データ送信料が発生する。 **▼データベース** RDSのMulti-アベイラビリティゾーン構成を採用することで、単一アベイラビリティゾーンで障害が発生したとしても、もう一方のアベイラビリティゾーンに自動で切り替わり、システムを継続稼働させることが可能である。 **▼ストレージ** 仮想サーバーやデータベースのバックアップ(スナップショット)は、S3に保管される。S3では、東京リージョン内の異なる3拠点以上にデータを自動複製・保存する為、災害に伴うデータ紛失のリスクを極小化される。
	日本国内での災害対策(オンプレミス環境のディザスターリカバリー先としてクラウドサービスを利用する場合)	オンプレミス環境のディザスターリカバリー先としてAWSを利用される場合、大きく以下の2つの構成が考えられる。 **▼バックアップ/コールドスタンバイ** オンプレミス環境にあるS3準拠の各種バックアップアプライアンス製品/統合バックアップソフトウエア製品/NAS製品/高速データ転送製品/Storage Gateway(VMware・Microsoft Hyper-Vベースのソフトウエアストレージのバーチャルアプライアンス)と連携して、バックアップデータをS3に格納することが可能である。オンプレミス環境が被災した場合は、S3から直接仮想サーバー(EC2)にデータをリストアしたり、統合バックアップソフトウエア製品を利用してデータリストアして、DNSを切り替えることで、AWS上にシステムをリカバリすることが可能となる。 ※S3準拠の各種バックアップアプライアンス製品/統合バックアップソフトウエア製品/NAS製品/高速データ転送製品の詳細については、AWS APNコンサルティングパートナー(SI)各社に相談可。 【参考 URL】 http://aws.amazon.com/jp/solutions/solution-providers-japan/ **▼ウォームスタンバイ/ホットスタンバイ** AWS環境上に仮想サーバー(EC2)を稼働させて、オンプレミス環境の各種サーバーとデータレプリケーションさせることで災害発生時のダウンタイムを極小化することが可能である。また、Route53のDNSラウンドロビン機能と組み合わせることで、オンプレミス環境とAWS環境のホットスタンバイ構成が実現可能となる。 ※データレプリケーションについては、各サーバーの用途・種別等によって、選択する手法や製品が異なる。
	グローバルレベルでの災害対策(日本国内で広域災害が発生した場合)	日本国内での広域災害を想定して、他国のリージョンを利用したグローバルレベルでの災害対策を鑑みる際、大きく以下の2つの構成が考えられる。 **▼バックアップ/コールドスタンバイ** 仮想サーバー(EC2)のイメージファイル(AMI)や仮想サーバー(EC2)のシステム/データ領域であるEBSボリュームのスナップショットデータを他国リージョンのS3に保管すること(リージョン間コピー)が可能である。日本国内で広域災害が発生した場合は、S3内に格納されたAMIから仮想サーバー(EC2)を起動したり、EBSスナップショットからEBSボリュームを作成し、各領域をアタッチして、DNSを切り替えることで、他国リージョンのAWS上にシステムをリカバリすることが可能となる。 **▼ウォームスタンバイ/ホットスタンバイ** 東京リージョンと同一構成を他国リージョンにも構築し、データレプリケーションさせた上で、Route53のDNSフェールオーバー機能を組み合わせてActive-Active構成とすることで、ホットスタンバイ構成が実現可能となる。 ※リージョン間を跨ぐトラフィックには、別途データ送信料が発生する。
1-6 持込可能ライセンス(BYOL)	Red Hat Enterprise LinuxのBYOL	Red Hat Enterprise Linuxに関するソフトウエアライセンスの持ち込み(BYOL)可否について、説明する。 **▼Red Hat Enterprise Linux** ・Red Hat Cloud Access契約をお客様とRed Hat社で締結することにより、購入したサブスクリプションライセンスの持ち込みが可能 ・Red Hat Cloud Access契約については、都度Red Hat社と調整が必要

	Microsoft製品のBYOL	Microsoft製品のソフトウエアライセンスの持ち込み(BYOL)可否については、以下の通りである。 **▼Windows Server** ・持ち込み不可 **▼Microsoft SQL Server** ・Standard/Enterprise Editonについては、EC2およびRDSともに持ち込み可能 ・ただし、有効なマイクロソフトソフトウエアアシュアランス（Microsoft Software Assurance/SA）契約の対象となるSQL Server ライセンスを持つマイクロソフトボリュームライセンス（Microsoft Volume Licensing/VL）のみが対象 ・1サーバーライセンスが1インスタンスに、1プロセッサライセンスが4仮想コアまでの1インスタンスに割り当てが可能 **▼その他** ・Microsoft SQL Serverと同様に、有効なマイクロソフトソフトウエアアシュアランス（Microsoft Software Assurance: SA）契約の対象となるSQL Server ライセンスを持つマイクロソフトボリュームライセンス（Microsoft Volume Licensing: VL）に限り、いくつかソフトウエアライセンスの持ち込みが可能。代表的なソフトウエアのみ以下に抜粋。 －Microsoft Exchange Server －Microsoft SharePoint Server －Microsoft Lync Server －Microsoft System Center Server －Microsoft Dynamics CRM －Microsoft Dynamics AX ・1サーバーライセンスが1インスタンスに、1プロセッサライセンスが4仮想コアまでの1インスタンスに割り当てが可能 ※1. "Microsoft SharePoint Foundation2010"については、ライセンス込みのEC2インスタンスも提供されている。 ※2. Microsoft製品のBYOLに関する最新情報については、『マイクロソフト製品使用権説明書(PUR)』を参照のこと。 【参考 URL】 https://www.microsoft.com/ja-jp/licensing/about-licensing/product-licensing.aspx
	Oracle製品のBYOL	Oracle製品のソフトウエアライセンスの持ち込み(BYOL)可否については、以下の通りである。 **▼Oracle Database (Processor License)** ・Editionによって、制約事項はあるものの、EC2およびRDSともに持ち込み可能 ・RDSでMulti-AZ構成の場合は、下記ライセンス数量の2倍のライセンスが必要 [Standard Edition One] ・8仮想コア以下のインスタンスが対象 ・仮想コア数を4で割り、小数点以下を切上げたカウント数分のライセンスが必要 [Standard Edition] ・16仮想コア以下のインスタンスが対象 ・仮想コア数を4で割り、小数点以下を切上げたカウント数分のライセンスが必要 [Enterprise Edition] ・仮想コア数に係数(0.5)を乗算したカウント数分のライセンスが必要 （※係数の0.5はIntelCPUを想定） **▼MySQL Server** ・16ECUごとに、"MySQL Standard/Enterprise Edition Subscription (1-4 soket server)"が1ライセンスずつ必要 ※1. RDSでは、[Community Edition]が利用可能 ※2. MySQL製品については コア係数の考え方がない為、CPU数を基準にライセンス数を算出 **▼Weblogic Server (Processor License)** ・Editionによって、制約事項はあるものの、持ち込み可能 [Standard Edition] ・16仮想コア以下のインスタンスが対象 ・仮想コア数を4で割り、小数点以下を切上げたカウント数分のライセンスが必要 [Enterprise Edition] ・仮想コア数に係数(0.5)を乗算したカウント数分のライセンスが必要 （※係数の0.5はIntelCPUを想定） 【参考 URL】 http://www.oracle.com/jp/corporate/pricing/index.html
	その他ソフトウエア製品のライセンス提供・BYOL	AWSでは、既に1,000をはるかに超える汎用ソフトウエア(OS/アプリケーションサーバー/データベース/セキュリティ製品など)・開発ツール(ログ分析/監視ソフト/テストツールなど)・ビジネスソフトウエア(CRM/eCommerceなど)のライセンス提供ならびにBYOLが可能となっており、今後もますます増加していくことが予想される。 まずは、AWS MarketplaceやAWSのWebサイトにて利用予定のソフトウエア製品のライセンス提供もしくはBYOLが可能なのかを確認する必要がある。 【参考 URL】 https://aws.amazon.com/marketplace/ref=brs_navhdr_header もし、AWS Marketplaceで該当しなかった場合は、ソフトウエア製品の開発・販売ベンダーに対して、以下の内容を確認する必要がある。 (1) AWS上でソフトウエア製品をインストールして動作させることが可能か？ (2) ソフトウエア製品のライセンス規約上、AWS上で動作させても問題が無いか？ (3) AWS上でソフトウエア製品を稼働させた場合の保守サポートが受けられるのか？ もし、AWS上でのソフトウエア製品のインストールならびに正常稼働が確認されているのに、ライセンス規約上や保守サポート上の問題が有る場合は、AWSからソフトウエア製品の開発・販売ベンダーに対して協力依頼を掛けることも可能である。
1-7 ネットワーク	プライベートIPアドレス	AWSにてEC2やRDSをご利用になる場合、Amazon VPC(Virtual Private Cloud)という仮想ネットワーク環境上で起動することになる。Amazon VPCにおいて、以下のRFC1918で定義されたIPv4のプライベートIPアドレスブロックから、お客様にてIPv4のプライベートIPアドレスを/16ネットマスクより小さい範囲で選択し、割り当てることが可能である。 ・10.0.0.0/8 ・172.16.0.0/12 ・192.168.0.0/16 ※VPC内に作成するサブネットについては、/28～/16ネットマスクの範囲内で指定する必要がある。

	パブリックIPアドレス	EC2にて、Webサーバー等の外部公開用サーバーを構築する際にElastic IPにてパブリックIPアドレスが採番される。具体的にお客様システムに採番されるパブリックIPアドレスの範囲は、適宜、AWSの開発者向けフォーラムにて、情報公開される。 **▼AWS開発者向けフォーラム** "Discussion Forums" -> "Category: Amazon Web Services" -> "Forum: Amazon Elastic Compute Cloud" -> "Announcement: EC2 Public IP Ranges" 【参考 URL】 https://forums.aws.amazon.com/ann.jspa?annID=1701 ※上記アナウンスでは、全てのリージョンのEC2で採番されるパブリックIPアドレスが記載・公開される。
	負荷分散(LoadBalancer)機能	AWSでは、負荷分散機能として、ELBが提供される。 **▼ELBの主な特徴** ・HTTP/HTTPS/TCP/SSL/カスタムの各プロトコルを管理可能 ・バックエンドのEC2インスタンスのリクエスト数やコネクション数を基に負荷分散(ラウンドロビン方式) ・健全なEC2にのみトラフィックを分配するヘルスチェック機能が有る ・ELB自体が負荷の増減に応じて自動スケール(※ELBがスケールする際にはIPアドレスが変化する為、ELBへのアクセスは必ずDNS名で指定する必要がある) ※AWSの分散型メモリキャッシュサービスである「ElastiCache」と組み合わせることで、仮想サーバーのローカルにセッション情報を保持せずに済むので、特定のサーバーがダウンしても別なサーバーで処理を継続することができ、ELB自体が複数のアベイラビリティゾーンに跨って配置されるため、複数のデータセンターに仮想サーバーを分散配置した上で負荷分散する構成が容易に実現できる。
	Firewall機能	AWSでは、セキュリティグループにてステートフルなインバウンドとアウトバウンドのフィルタを使って、EC2/RDSインスタンスを防御することが可能である。また、ネットワークアクセスコントロールリストにて、個別のサブネットに対してのインバウンドとアウトバウンドへINとOUTのアクセスを制御することも可能である。
	リモートアクセス	Amazon VPCへのリモートアクセスは、標準ではインターネットVPN(IPSec-VPN)もしくは専用線/閉域網接続(Direct Connect)の2種類から選択可能である。 **▼インターネットVPN (IPSec-VPN)** ・お客様側のソフトウエアVPNもしくはVPN機器を利用して接続 ・静的/動的ルーティングの両方をサポート (※ただし、機器仕様に制限有り) ・「接続拠点数・1時間単位の料金」で課金 **▼専用線/閉域網接続 (Direct Connect)** ・「各接続ポート(1Gbpsもしくは10Gbps)の1時間当たりの料金」と「データ転送量(1GB単位)ベースの料金」で課金 ※1. リモートアクセス(回線サービスを含む)に関する詳細は、AWS APNコンサルティングパートナーおよびAPNソリューションプロバイダー各社に相談可。 【参考 URL】 http://aws.amazon.com/jp/solutions/solution-providers-japan/ ※2. AWSの標準サービスでは、SSL-VPNによるリモートアクセス機能は提供されていません。SSL-VPNによるリモートアクセスが必要な場合は、専用の仮想アプライアンスを用意する等の個別構築することも可能である。
	他システム連携	オンプレミス環境や他のパブリッククラウドサービスとAWS環境は、インターネットVPN(IPSec-VPN)や専用線/閉域網接続(Direct Connect)経由で、IPアドレスを変えること無く、シームレスにシステム間連携が可能である。 また、HULFTやDataSpiderなどデータ転送ソフトと組み合わせることで、転送時のデータ整合性チェックや転送エラー発生時の自動再送を行うことも可能となる。 ※HULFTもDataSpiderも、AWSへのライセンス持込(BYOL)が可能である。
1-8 その他	時刻同期(NTP)	EC2でAmazon Linuxインスタンス、Windows系インスタンスを選択する場合、標準で以下のNTPサーバーを時刻同期の参照値として設定されている。 **▼AmazonLinuxインスタンスの場合** 以下のNTPサーバと時刻同期する設定となっている。 ― "0.amazon.pool.ntp.org" ― "1.amazon.pool.ntp.org" ― "2.amazon.pool.ntp.org" ― "3.amazon.pool.ntp.org" **▼Windows系インスタンスの場合** "time.windows.com"と時刻同期する設定になっている。 なお、その他OSの場合、時刻同期プロセス(ntpdなど)がデフォルトでインストールされていない場合もあるため、構築時は注意が必要である。
	外部DNS機能	AWSでは、外部DNS機能のサービスとして、Route53が利用可能である。 **▼Route53の主な特徴** ・全世界のエッジロケーションにてAnycastネットワークを使用、エンドユーザーからもっとも近いエッジロケーションが応答 ・標準では、ユーザーあたり100ホストゾーン(ドメイン)まで/1ホストゾーン10,000レコードまでが登録可能(※上限緩和申請を提出することで上限変更も可能) ・サポートされているレコード:A(IPv4)/CNAME/MX/AAAA(IPv6)/TXT/PTR(ポインター)/SRV(Service locator)/SPF(Sender Policy Framework)/NS/SOA(管理情報の始点レコード) ・ルーティングポリシー:Simple/Weighted(重みづけラウンドロビン)/Latency(レイテンシーベースルーティング)/Failover/Geolocation ・DNSヘルスチェック機能・フェールオーバー機能有り ・登録したホストゾーン数、クエリ数、ヘルスチェック件数に応じて課金が発生 ※Route53を利用しない場合は、個別にbindなどでDNSサーバーを構築することも可能である。
	内部DNS機能	AWSでは、サブネット内に自動的に内部DNSサーバーが作成され、各インスタンスは、自動的に内部DNSホスト名が付与される。(凡例:ip-xxx-xxx-xxx-xxx.ap-northeast-1.compute.internal) ※キャッシュサーバーが必要な場合は、EC2での個別構築が必要となる。
	CDN	AWSでは、CDNサービスとして、CloudFrontが利用可能である。 **▼CloudFrontの主な特徴** ・全世界のエッジロケーションにキャッシュされ、エンドユーザーからもっとも近いエッジロケーションが応答 ・Webコンテンツ(http/https)ならびに動画ストリーミング(RTMP)の配信が可能 (※WebサイトまたはWebアプリケーション全体の配信、ソフトウエアや大容量ファイルの配布、メディアファイルの配信の用途で使用可能) ・オリジンサーバーは、EC2/S3/ELBから選択が可能 ・データ転送のトラフィック量とリクエスト数に応じて課金が発生 ・全てのログファイルは、S3に保存

1-9 責任範囲	利用者とサービス提供者の責任範囲	一般的に(AWSに限らず)クラウドサービスを利用する場合は、サービスメニューに提示された内容とその責任範囲に対して、設定されたSLAに基づいてサービスを利用することになる。ここでは、AWSにおける責任範囲について、説明する。 **▼AWS責任範囲** ファシリティ/物理セキュリティ/物理インフラ(サーバー・ストレージ)/ネットワークインフラ/仮想インフラの各種システムリソースおよび各種AWSサービスの提供 **▼利用者責任範囲** アカウント管理/ネットワーク設定/セキュリティグループ/OSファイアウォール/OS/ミドルウエア/アプリケーションの設計・構築・運用・保守・管理 利用者責任範囲の業務の支援を得るために、AWSでは認定パートナー制度(APNコンサルティングパートナー(SI))を活用することが推奨される

第2節　可用性／信頼性要件

項目	要件	回答
2-1 稼働率	稼働率に基づくサービスレベル保証(SLA)	AWSでは、いくつかのサービスにおいて、稼働率が保証されている。 ペナルティが設定されているSLAについて、説明する。 **▼EC2** ・『月間使用時間割合』(1ヶ月間でEC2またはEBSがリージョン内で使用不能状態になった時間分の割合を100%から減算)が99.95%以上。 ・99.95%未満なら、割合に応じてペナルティ(サービスクレジット率)有り。 【参考 URL】 http://aws.amazon.com/jp/ec2-sla/ **▼RDS** ・Multi-AZインスタンスの『月間使用時間割合』が99.95%以上。 ・99.95%未満なら、割合に応じてペナルティ(サービスクレジット率)有り。 【参考 URL】 http://aws.amazon.com/jp/rds/sla/ **▼S3/CloudFront** ・『月間使用時間割合』(月間請求期間内における5分間のエラー率の平均を100%から減算)が99.9%以上。 ・99.9%未満なら、割合に応じてペナルティ(サービスクレジット率)有り。 【参考 URL】 [S3] http://aws.amazon.com/jp/s3-sla/ [CloudFront] http://aws.amazon.com/jp/cloudfront/sla/ ※ S3は、99.999999999%の堅牢性と99.99%の可用性を提供するようにサービス設計されている。(ただし、堅牢性と可用性のSLAに対するペナルティは無し) **▼Route53** 『使用可能時間割合』(毎月の請求期間にRoute53が利用者のDNSクエリ応答に失敗しなかった割合)が100%。DNSクエリ応答に失敗した時間が5分以上なら、失敗した時間に応じて、ペナルティ(サービスクレジット)有り。 【参考 URL】 http://aws.amazon.com/jp/route53/sla/ ミッションクリティカルシステムやプライムシステムに区分されるようなシステムでは、各サービス単一のSLAでは要件を満たせない可能性が有る為、個別に耐障害性をより強く意識した構成を検討する必要がある。
2-2 可用性	アプリケーション層	AWSでは、アプリケーション層の可用性を高めるための機能が用意されている。 **▼AMI** ・OS/ミドルウエア/アプリケーションを含めたサーバーインスタンスをテンプレートとして定義することが可能 ・故障または劣化したEC2インスタンスの交換はAMIからインスタンスを起動するだけで可能 ・AMIのOS/ミドルウエア/アプリケーション自体を最新状態に保つための施策として、インスタンスが起動次第ブートストラップスクリプトを実行して必要なソフトウエアコンポーネントとコンテンツをインストールすることも可能 **▼EIP** ・インスタンスのIPアドレスにEIP(固定IPアドレス)を使用することで、インスタンスの切り替え時に付け替えることで瞬時に切り替えることが可能 ・常にスペアのインスタンスを用意しておき、故障が生じた時に代替インスタンスにフェールオーバーすることも可能 **▼Multi-AZ構成** ・複数のアベイラビリティゾーンにEC2インスタンスを配置し、ELB(ロードバランサー)で常に正常なインスタンスで処理させるよう構成することで耐障害性の高いアプリケーションを構築可能 **▼Auto Scaling** ・Auto Scaling機能を利用することで、自動的に故障を検知し、代替インスタンスを起動させるような、N+1冗長構成を実現することが可能である。 **▼EC2 + EC2** ・EC2上で動作サポートするサードパーティーのクラスタソフトウェアの普及に伴い、従来のオンプレミス環境と同様なDBのクラスタを構成することが可能。(代表的なクラスタソフトウェア：LifeKeeper、CLUSTERPRO)
	データベース層	AWSでは、データベース層の可用性を高めるための機能が用意されている。 **▼RDS(リレーショナルデータベースサービス)** ・汎用的なリレーショナルデータベースサービスであり、複数のアベイラビリティゾーンへの自動レプリケーション構成の構築ができ、障害時にはフェールオーバーが可能 ・自動・手動バックアップとディザスターリカバリー機能、手動スナップショットとクローン機能を利用可能 ・インスタンス停止は必要だが、スケールアップが容易に可能 ・RDS(MySQL)はリードレプリカ機能でReadのスケールアウトが可能 **▼DynamoDB** ・NoSQL型のデータベースサービスであり、複数アベイラビリティゾーンへの自動レプリケーション構成の構築ができ、障害時にはフェールオーバーが可能 ・ReadとWriteの双方のスケールアウトが可能 **▼EC2 + DB** ・DBソフトウエアのバージョンや構築・設定を自由に行いたい場合は、EC2上のDBを構築することが可能だが、可用性を高める構成は従来通りの方法で実施する必要がある。
	ストレージ	AWSの各種ストレージサービスは可用性を考慮された設計になっている。 **▼EBS** ・内部的に冗長化された構成となっている ・EBSボリュームの特定時点のスナップショットをS3に保存可能 ・作成したスナップショットをリージョン内コピー、リージョン間コピーが可能 ・OSレベルのソフトウエアRAIDを構成することも可能 ※ソフトウエアRAIDで構成していて、EBSスナップショットを取得する場合、RAID構成は考慮されず、あくまでEBSボリューム単位でのスナップショットになる点について、注意する必要がある。 **▼S3 / Glacier** ・保存したデータをリージョン内の複数のアベイラビリティゾーンに自動複製(99.999999999%の高い耐久性) ・障害検知とデータ修復機能を有する ・計画停止なし

	ファシリティ	ファシリティに関する可用性という観点でも、AWSにていくつかの対策が施されている。 **▼データセンター(アベイラビリティゾーン)構成** ・1つのリージョンは、複数のアベイラビリティゾーンから構成される ・各アベイラビリティゾーンは都市地域内で物理的に40-60km程度分離されている ・複数のアベイラビリティゾーンで同時に洪水・浸水等の影響が及ばないような場所に立地している **▼物理的セキュリティ** ・ビデオ監視カメラ、最新鋭の侵入検出システムを配備 ・物理的なアクセス制御として、2要素認証を最低2回用いている **▼防火・温湿度管理** ・自動火災検出システム(煙検出センサー)・鎮火装置を設置 ・温度・湿度を監視・コントロール **▼電力設備** ・異なる電力供給施設から異なる配管網を経由して個別に電力供給される ・電力システムは完全冗長化構成 ・電力障害時は、無停電電源装置(UPS)と発電機がバックアップ電力を供給 **▼回線設備** ・冗長的に複数のTier-1プロバイダーに接続 ※AWSでは、機密保持契約(NDA)を締結することでSOC1 TypeIIレポートのコピーを提供可能
2-3 バックアップ方式/範囲	実現方式/対象範囲/データ整合性	AWS環境における代表的なバックアップの方式として、以下の4種類が考えられる。 **▼各種サードパーティ製品と組み合わせたS3/Glacierへのバックアップ** ・実現方式: S3準拠のバックアップアプライアンス製品/統合バックアップソフトウエア製品/NAS製品/高速データ転送製品といった各種サード パーティ製品と利用・連携して、S3/Glacireへバックアップ ・対象範囲: オンプレミス環境ないしAWS環境上の、特定のファイル/ディレクトリ等のデータバックアップ、システムバックアップ、仮想サーバーのイメージバックアップ、スナップショットデータの差分バックアップなど ・データ整合性: システムとしての静止点を確保した製品・設定を選択すれば、整合性は確保可能。 ※対象範囲とデータ整合性は、各種サード パーティー製品の仕様と設定により異なる。 **▼Storage Gateway経由でのS3へのバックアップ** ・実現方式: オンプレミス環境上のStorage Gateway(VMware・Microsoft Hyper-Vベースのソフトウエアストレージのバーチャルアプライアンス)を利用して、S3へバックアップ ・対象範囲: オンプレミス環境にあるシステムのD2Dバックアップ(統合バックアップソフトウエア製品等による特定のファイル/ディレクトリ等のデータバックアップ、仮想サーバーのイメージバックアップなど) ・データ整合性: システムとしての静止点を確保した製品・設定を選択すれば、整合性は確保可能。 ※対象範囲とデータ整合性は、各種サード パーティ製品の仕様と設定により異なる。 **▼EBSスナップショット** ・実現方式: EC2(仮想サーバー)に割り当てられたEBSボリューム毎にスナップショットを取得 ※EBSスナップショットは、他リージョンへのコピーも可能。 ・対象範囲: AWS環境上の仮想サーバーのシステム/データ領域(EBSボリューム)単位 ・データ整合性: 一時的に仮想サーバーを停止する等、システムとしての静止点を確保した上で、EBSスナップショットを取得すれば、整合性は確保可能。 **▼AMIによるイメージバックアップ** ・実現方式: EBSスナップショットをベースにして仮想サーバーイメージを作成・保管 ※AMIは、他リージョンへのコピーも可能。 ・対象範囲: AWS環境上の仮想サーバーのシステム領域 ・データ整合性: 一時的に仮想サーバーを停止する等、システムとしての静止点を確保した上で、EBSスナップショットを取得したものからAMIを作成すれば、整合性は確保可能。
2-4 ディザスタリカバリ方式/範囲	実現方式/利点/注意点	AWSで実現できるディザスタリカバリの方式として、以下の4種類が考えられる。 **▼S3/Glacierへのバックアップ+リストア** ・実現方式: S3準拠のバックアップアプライアンス製品/統合バックアップソフトウエア製品/NAS製品/高速データ転送製品/Storage Gateway(VMware・Microsoft Hyper-Vベースのソフトウエアストレージのバーチャルアプライアンス)と連携・利用して、S3/Glacierへバックアップ ・リストア時: オンプレミス環境もしくはAWS環境に実施 ・利点: 構成が最もシンプル、データの外部保管先の課金が従量制 ・注意点: コストが廉価な反面、災害発生時の復旧には最も時間を要する方式 **▼コールドスタンバイ** ・実現方式: 事前にAWS上にシステムイメージ(もしくは統合バックアップソフトウエア製品のマネージャー)を用意し、S3準拠のバックアップアプライアンス製品/統合バックアップソフトウエア製品/NAS製品/高速データ転送製品/Storage Gateway(ソフトウエアストレージのバーチャルアプライアンス)と連携・利用して、S3/Glacierへバックアップ、EBSスナップショット/AMIを他のリージョンにコピー ・リストア時: AWS環境に実施 ・利点: 構成が比較的シンプル、災害発生時のみAWS上でシステムが稼動するため費用対効果は高い ・注意点: コールドスタンバイしているAWS側のシステムメンテナンス・定期的な切替テストは実施必要、切替・リストアのオペレーションが煩雑化する恐れがある **▼ウォームスタンバイ** ・実現方式: AWS上で常時最小構成で稼働し、ソフトウエア製品によるデータ同期を実施。災害発生時に必要なキャパシティに変更。(※リストアは基本的に不要) ・利点: 災害発生時の切替オペレーションが比較的容易 ・注意点: (オンプレミス環境のスタンバイがAWS上になる場合)VPNもしくは専用線接続が必須、システム次第ではこの方式は実現不可となる場合がある **▼マルチサイトホットスタンバイ** ・実現方式: オンプレミス環境もしくはAWS環境との冗長構成を組み、災害発生時はAWS環境のみ片系運転(※リストアは基本的に不要) ・利点: 災害発生時の切替が極小化、災害発生時でもAWS環境のキャパシティを考慮する必要無し ・注意点: (オンプレミス環境のスタンバイがAWS上になる場合)VPNもしくは専用線接続が必須、実現できるシステムに限りが有る

2-5 ディザスタリカバリ復旧目標	RPO（目標復旧地点）/RTO（目標復旧時間）/コスト感	AWSで実現できるディザスタリカバリの4種類の方式における、RPO(目標復旧地点)・RTO(目標復旧時間)・コスト感について記載する。 **▼S3/Glacierへのバックアップ＋リストア** ・RPO：直前のS3/Glacierへのバックアップ取得時点 ・RTO：72時間以上 ・コスト感：最も安価 **▼コールドスタンバイ** ・RPO：直前のコールドサイトへのバックアップ取得時点 ・RTO：30分 ～ 72時間 ・コスト感：比較的安価 **▼ウォームスタンバイ** ・RPO：直前のデータ同期時点 ・RTO：15秒 ～ 30分 ・コスト感：比較的高価 **▼マルチサイトホットスタンバイ** ・RPO：直前のデータ同期時点 ・RTO：常時 ～ 15秒 ・コスト感：最も高価 ※上記RTOについては、あくまで「目安」で有り、実際の時間は、接続回線の状態・データ量・バックアップ/レプリケーションソフトウエアの仕様等々に応じて、大きく異なる。

第3節　性能／拡張性要件

項目	要件	回答
3-1 CPU 性能（vCPU 数）	CPU数/増減単位	EC2は複数のインスタンスタイプが提供されており、それぞれのインスタンスタイプはさまざまなCPU、メモリ、ストレージ、ネットワークキャパシティーの組み合わせによって構成されている。 東京リージョンでは1仮想コア～32 仮想コアのインスタンスタイプが提供されている。 仮想コア数の変更はインスタンスタイプを変更することで可能となる。インスタンスタイプを変更するにはシステムの停止が必要である。 【参考URL】 http://aws.amazon.com/jp/ec2/instance-types/
3-2 メモリ量	メモリサイズ/増減単位	CPU性能と同じく、EC2で複数提供されているインスタンスタイプはさまざまなメモリサイズで構成されている。 東京リージョンでは0.613～244GiBのインスタンスタイプが提供されている。 メモリサイズの変更はインスタンスタイプを変更することで可能となる。インスタンスタイプを変更するにはシステムの停止が必要である。 【参考URL】 http://aws.amazon.com/jp/ec2/instance-types/
3-3 ディスク量/性能	ディスクサイズ/増減単位/IOPS	EC2に直接アタッチ可能なブロックストレージとして以下の2つのストレージが提供されている。 **▼インスタンスストア** EC2 インスタンスで使用するための一時ストレージを提供する。ほとんどのインスタンスタイプには、このインスタンスストアボリュームが標準で付属されている。インスタンスストアボリュームは最大 48 TB までで、インスタンスタイプによって異なるが、基本的には大きなインスタンスタイプほどサイズが大きくなる。また中には高性能なSSDを搭載したタイプもある。インスタンスを停止／起動するとインスタンスストアボリュームに保存されていたデータは消失してしまうことになる。またデタッチして他のインスタンスに再アタッチすることはできない。一時的なデータの保存に適している。 **▼EBS** ネットワークアタッチ型であり、EC2 インスタンスの存続期間とは独立した永続性を持つ。 1 GB～1 TB のストレージボリュームを作成して、EC2 インスタンスにデバイスとしてアタッチすることができる。 複数のEBSボリュームを同じインスタンスにアタッチすることが可能である。 アタッチ後は、ハードドライブやその他のブロックデバイスと同様に、マウントされたデバイスとして認識される。 サイズを変更（減少、増加）する際は対象EBSボリュームのデタッチ、アタッチが必要になる。 EBSボリュームは作成時に明示的に指定した特定のアベイラビリティゾーンに配置され、そのアベイラビリティゾーン内のインスタンスにアタッチすることが可能である。 複数のボリュームをアタッチしてストライピングすることによりI/O性能を高めることも可能である。 また、EBSボリュームには、以下のとおり、General Purposeボリューム、Provisioned IOPSボリューム、Magneticボリュームの3種類が提供されいている。 **▼General Purposeボリューム** General Purposeボリュームは、システムブートボリューム、小規模から中規模のデータベースに適している。 General Purposeボリュームは、最大30分間にわたって最大 3,000 IOPSまでバーストできる機能および1 GiBあたり3 IOPSのベースパフォーマンスが実現される。IOPSのバースト期間およびIOPSのパフォーマンスレベルは、ボリュームサイズに応じて毎秒取得されるI/Oクレジットの未使用量に依存する。 **▼Provisioned IOPSボリューム** Provisioned IOPSボリュームは、予測可能な高パフォーマンスを実現するよう設計されており、大量の I/O が発生するワークロード（データベースなど）に適している。Provisioned IOPSボリュームでは、ボリューム作成時に IOPS レートを指定でき、ボリュームの存続期間中はそのレートに従ってIOPS性能がプロビジョニングされる。 2013年11月時点では、Provisioned IOPSボリュームあたり最大 4,000 IOPS がサポートされている。複数のボリュームをまとめてストライピングすることにより、EC2 インスタンスあたり数千 IOPS をアプリケーションに対して提供することが可能である。 EC2の「EBS 最適化インスタンス」を使用するとEC2インスタンスとProvisoned IOPSボリュームの間でインスタンスタイプに応じて500 Mbps または 1,000 Mbps のスループットを実現できる。「EBS 最適化インスタンス」にアタッチされたProvisioned IOPSボリュームは、プロビジョニングされた IOPS の±10% 以内のパフォーマンスを 99.9% の確率で発揮するように設計されている。 **▼Magneticボリューム** Magneticボリューム（旧スタンダードボリューム）は、アクセスがそれほど頻繁に行われず、低ストレージコストが重視されるワークロードに適している。Magneticボリュームの平均パフォーマンスは約 100 IOPS であり、ベストエフォートで数百 IOPS のバーストも可能である。 【参考URL】 http://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSVolumeTypes.html
3-4 ネットワーク帯域/速度	帯域	AWSのサービス内でのネットワーク帯域は保証されていない。 但し、インスタンスタイプによってはクラスターネットワークをサポートしている。クラスタープレイスメントグループに登録されたインスタンスは、クラスター内の全インスタンス間で高帯域（10Gbps）で低レイテンシーのネットワークを提供する論理クラスターに配置される。クラスターネットワークは、特に並列プログラミングに標準的な MPI ライブラリーを使用する、高性能分析システム、多くの科学および工学応用に適している。 【参考URL】 http://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/using_cluster_computing.html
3-5 ネットワーク機器の持ち込み/ ネットワーク利用	ネットワーク機器の持ち込み/専用線の利用可否	AWSへネットワーク機器等を持ち込むことはできない。 ネットワークに関してはユーザーネットワークと専用線で接続するDirect Connectというサービスが提供されている。Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができる。これにより、ネットワークのコストを削減し、帯域幅のスループットを向上させることが可能となる。Direct Connect は、1 Gbps および 10 Gbps の接続を提供し、より多くの容量が必要な場合には、容易に複数の接続をプロビジョニングすることが可能である。 【参考URL】 http://aws.amazon.com/jp/directconnect/

第4節　セキュリティ要件

項目	要件	回答
4-1 ユーザー認証/利用制限 [IaaS/PaaS]	認証方式、アクセス制限/特権管理、不正時のアカウントロックの範囲/内容	IAMを使用すると AWS サービスおよびリソースへのアクセスをコントロールすることが可能である。 IAM を使用すると、AWS のユーザーとグループを作成および管理し、権限を使用して AWS リソースへのアクセスを許可および拒否することが可能である。 IAMは社内ディレクトリサービスと AWS のサービスとの間の認証フェデレーションが可能である。 また、AWS Webサイトにサインインする際に多要素認証デバイス(MFAデバイス)による認証を行うことも可能である。 その他、OSレベル、アプリケーションレベルの認証については、従来どおりの方式が利用可能である。 【参考URL】 http://aws.amazon.com/jp/iam/
4-2 データセキュリティ/完全性	データ暗号化方式(伝送データ)	ELBは標準で証明書管理機能を持っており、以下の設定が可能である。 ・ELBでSSL TerminationしバックエンドのEC2とSSLなし ・ELBでSSL TerminationしバックエンドのEC2と別途SSL また、SSLをバイパスしてバックエンドのEC2へTCPで通信することも可能である。 【参考URL】 http://aws.amazon.com/jp/elasticloadbalancing/
	データ暗号化方式(蓄積データ)	EBSボリュームおよびそれに関連づけられたスナップショットを暗号化する仕組みが提供されている。 S3については、サーバー側の暗号化(SSE)、またはS3に格納する前に独自の暗号化ライブラリを使用してデータを暗号化することが可能である。 【参考URL】 http://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html http://aws.amazon.com/jp/s3/
4-3 ネットワーク領域の保護/分離	ネットワーク制御方式	VPCを使用して、AWSクラウド環境の論理的に分離したセクションをプロビジョニングし、ユーザーが定義する仮想ネットワークで AWS リソースを起動することができる。独自の IP アドレス範囲の選択、サブネットの作成、ルートテーブル、ネットワークゲートウェイの設定など、仮想ネットワーク環境をユーザーが設定することが可能である。 例えば、インターネットとのアクセスが可能なWebサーバーのパブリックサブネットを作成し、データベースやアプリケーションサーバーなどのバックエンドシステムをインターネットとのアクセスを許可していないプライベート サブネットに配置できる。セキュリティグループやネットワークアクセスコントロールリストなどの複数のセキュリティレイヤーを活用し、各サブネットの EC2 インスタンスへのアクセスをコントロールすることができる。 加えて、社内ネットワークと自分の VPC 間にハードウエア Virtual Private Network(VPN)接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することが可能である。 【参考URL】 http://aws.amazon.com/jp/vpc/
	ファイアウォール機能	以下の2つのファイアウォール機能が提供されている。 **▼セキュリティグループ** EC2、RDS、ElastiCacheのファイアウォールとして動作し、インバウンドトラフィックとアウトバウンドトラフィックの両方をインスタンスレベルでコントロールする(ステートフル)。 インバウンドトラフィックはデフォルトで全て拒否に設定されている。トラフィックはプロトコル、サービスポート、ソース/宛先IPアドレスにより制限可能である。 **▼ネットワークアクセスコントロールリスト(ネットワークACL)** ネットワークACLはVPCの機能の1つである。 ネットワークACLはそれに関連付けられたサブネットのファイアウォールとして動作し、インバウンドトラフィックとアウトバウンドトラフィックの両方をサブネットレベルでコントロールする(ステートレス)。 トラフィックはプロトコル、サービスポート、ソース/宛先IPアドレスにより制限可能である。 【参考URL】 http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_Security.html
	ネットワーク領域の保護	ネットワークの保護の方法としては以下の2つがある。 両方式ともに既存データセンターのオンプレミス環境等との接続に有効である。 **▼VPN** AWS上に構築したVPCに社内等からVPN接続して閉域網でAWSを利用することが可能である。AWSが社内インフラの一部のように見えるようになる。社内側にハードウエアVPN装置を別途準備する必要がある。 **▼Amazon Direct Connect** IEEE 802.1Q準拠のVLANを使用して、データセンターやオフィスとAWSとの間を専用線(1 Gbps および 10 Gbps)で接続する。 相互接続ポイント(東京都品川区)まで専用線を直接接続するか、通信事業者、AWSパートナー各社が提供する接続サービスを利用して接続することができる。 【参考URL】 http://aws.amazon.com/jp/vpc/ http://aws.amazon.com/jp/directconnect/
4-4 侵入検知/不正追跡	IDS/IPS/WAFの設置等	標準では提供されていないが、OSS、サード パーティー製品等を使用して個別に構築することが可能である。 【参考URL】 http://aws.amazon.com/jp/security/
	ログの取得/保管/保護の範囲/内容	AWS CloudTrailを使用するとManagement Console、AWS Command Line InterfaceのAWS APIに対するコールを記録し、指定したS3バケットにログファイルを保存することができる。 特定のユーザーがある期間に行った操作、特定のリソースに対してどのAWSユーザーが操作を実行したか、ある操作に対してどのIPアドレスから行われたかを確認することが可能である。 また、不適切な権限のため実行が拒否されたAPIコールについても確認することが可能である。 また、OS、ミドルウエア、アプリケーション等の監査ログについては従来通り個別に取得することができる。 【参考URL】 http://aws.amazon.com/jp/cloudtrail/
4-5 ネットワークセキュリティ	DoS/DDoS 攻撃対策	インフラに対する分散サービス妨害(DDoS)攻撃への対応として標準的な緩和策は導入されている。 DoS/DDoS攻撃の対応をユーザー側で行うことも可能である。 【参考URL】 http://aws.amazon.com/jp/security/

	介入者（MITM）攻撃対策	全ての AWS API は、サーバー認証を提供する、SSL で保護されたエンドポイント経由で利用可能である。EC2 AMI は新しい SSH ホスト証明書を、最初のブート時に自動的に生成し、それらをインスタンスのコンソールに記録する。その後、ユーザーはセキュリティで保護されたAPI を使用してコンソールを呼び出し、最初にインスタンスにログインする前にホスト証明書にアクセスする。ユーザーは、AWS とのやり取りすべてにおいて SSL の使用が推奨されている。 【参考URL】 http://aws.amazon.com/jp/security/
	IPスプーフィング対策	EC2 インスタンスは、なりすましを受けたネットワークトラフィックを送信できない。AWSの管理された、ホストベースのファイヤウォールインフラストラクチャは、それ自身以外のソースIPまたはMACアドレスを有するトラフィックの送信を、インスタンスに許可しない。 【参考URL】 http://aws.amazon.com/jp/security/
	ポートスキャニング対策	EC2 の顧客による許可のないポートスキャンは、AWS のポリシーに違反する。ポリシーの違反は深刻に受け止められ、報告された違反は全て調査されることになる。許可のないポートスキャニングが検出される場合、それは停止されブロックされる。EC2 インスタンスの入力ポートは全てデフォルトで閉じられており、ユーザーによってのみ開くことが可能である。ユーザーは適切なセキュリティ手段を講じて、アプリケーションにとって重要なリスニングサービスを、未許可のポートスキャンに発見されることから保護する必要がある。 AWSに事前申請することにより、ユーザー自身のインスタンスに対してポートスキャンを実施することが可能である。 【参考URL】 http://aws.amazon.com/jp/security/
	第三者によるパケットスニッフィング対策	無差別モード（プロミスキャス・モード）で実行中の仮想インスタンスが、異なる仮想インスタンス向けのトラフィックを受信したり「傍受」することは不可能となっている。ユーザーは自らのインターフェイスを無差別モードにすることがはできるが、ハイパーバイザーが宛先でないインスタンスにトラフィックを伝送することはない。物理的に同一のホスト上に位置する、同一のユーザーによって保有される2つの仮想インスタンスであっても、互いのトラフィックを傍受することはできない。ARP キャッシュポイズニングなどの攻撃は、EC2 および Amazon VPC では機能しない。EC2 は、意図せず、または悪意をもって他者のデータを閲覧しようとする利用者に対して、豊富な防止対策を提供しているが、一般的にはユーザーは重要なトラフィックを暗号化する必要がある。 【参考URL】 http://aws.amazon.com/jp/security/
4-6 ウィルス/マルウエア対策	ウィルス/マルウエア対策	標準では提供されていないが、OSS、サード パーティー製品等を使用して個別に構築することが可能である。 【参考URL】 http://aws.amazon.com/jp/security/
4-7 物理環境の専有	物理環境の専有	通常、AWSのEC2環境ではハイパーバイザー上で互いに分離された個々のゲストOSが稼動している。 ハイパーバイザーは個々のゲストOSを互いに分離することで、同一物理マシン上であっても互いに干渉しないように制御されている。 但し、規制や条約等の理由により他ユーザーから物理的な分離が必要になる場合がある。 その場合、EC2の「ハードウエア占有インスタンス（EC2 Dedicated Instance）」が利用可能である。 ハードウエア占有インスタンスはAmazon VPC単位もしくは特定のAmazon VPC内のインスタンス単位に設定でき、EC2 コンピューティングインスタンスをハードウエアレベルで確実に分離しながら、オンデマンド伸縮自在なプロビジョニング、従量課金制、プライベートの独立した仮想ネットワークといった、Amazon VPC と AWS クラウドの利点を生かすことが可能である。 【参考URL】 http://aws.amazon.com/jp/security/
4-8 データセンターのセキュリティ	物理的セキュリティ	AWS のデータセンターは、外部からはそれとはわからないようになっている。ビデオ監視カメラ、最新鋭の侵入検出システム、その他エレクトロニクスを使った手段を用いて、専門のセキュリティスタッフが、建物の入り口とその周辺両方において、物理的アクセスを厳密に管理されている。権限を付与されたスタッフが2要素認証を最低2回用いて、データセンターのフロアにアクセスすることになっている。全ての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添われることになっている。 【参考URL】 http://aws.amazon.com/jp/security/
	電力	AWSのデータセンターの電力システムは、完全に冗長性を持ち、運用に影響を与えることなく管理が可能となっている。1日24時間体制で、年中無休で稼動している。施設内で重要かつ不可欠な負荷に対応するために、電力障害時には無停電電源装置（UPS）がバックアップ電力を供給している。データセンターは、発電機を使用して施設全体のバックアップ電力を供給している。 【参考URL】 http://aws.amazon.com/jp/security/
	データセンターの可用性	各アベイラビリティゾーンは、独立した障害ゾーンとして設計されている。各アベイラビリティゾーンは、一般的な都市地域内で物理的に分離されており、洪水の影響が及ばないような場所にある（洪水地域の分類はリージョンによって異なる）。個別の無停電電源装置（UPS）やオンサイトのバックアップ装置に加え、シングルポイントの障害の可能性を減らすために、別々の電力供給施設から異なる配管網を経由して、個別に電力供給が行われている。これらは全て、冗長的に、複数の Tier-1 プロバイダーに接続されている。 ユーザーは複数のアベイラビリティゾーンにアプリケーションを配信することによって、自然災害やシステム障害など、ほとんどの障害に対して、その可用性を保つことができる。 【参考URL】 http://aws.amazon.com/jp/security/
	ストレージデバイスの廃棄	AWSではストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが実行されている。AWS は、DoD 5220.22-M（「National Industrial Security Program Operating Manual（国立産業セキュリティプログラム作業マニュアル）」）または NIST 800-88（「Guidelines for Media Sanitization（メディア衛生のためのガイドライン）」）に詳細が記載されている技術を用いて、廃棄プロセスの一環としてデータは破棄されている。これらの手順を用いてハードウエアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊される。 【参考URL】 http://aws.amazon.com/jp/security/

	データの保存場所	リージョン間のデータのレプリケートはユーザーが能動的に実行しない限り行われない。利用可能な地理的司法管轄域内のリージョンをユーザーが選択することによって、欧州データプライバシー指令のような、地域に依存する個人情報およびコンプライアンス要件に適合する堅牢な環境が提供される。 リージョン間の通信はパブリックなインターネットインフラストラクチャを介して行われる。重要なデータをリージョン間で送受信する場合は、ユーザが適切な暗号化手段を使用して保護することが可能である。 【参考URL】 http://aws.amazon.com/jp/security/

第5節　運用要件

項目	要件	回答
5-1 運用スケジュール	インフラの運用時間帯	AWSでは、グローバルレベルで24時間365日体制にてサービス提供されており、ミッションクリティカルシステムでもご利用いただくことが可能である。 ※その一方で、コスト最適化の一環として、平日夜間帯や土日祝日等のシステム利用が見込まれていない、もしくはアクセスが少ないタイミングで、システムリソースを意図的に停止・縮小させる事も可能である。
5-2 計画停止スケジュール	実施頻度/期間、事前アナウンス	AWSでは、定期的な計画停止作業はない。 一方で、必要に応じて、不定期でメンテナンス作業は適宜実施される。メンテナンス作業時は、事前に利用者に対して、Webコンソール経由もしくはメールにて通知される。 ※月間の平均稼働率として99.95%以上を求められるミッションクリティカルシステムやプライムシステムに区分されるようなシステムでは、メンテナンス作業の影響を受けないようなシステム構成を予めご検討されることを推奨する。
5-3 運用窓口	言語、問い合わせ方法/対応時間、回答リードタイム、アーキテクチャーサポートレベル	AWSにおける運用サポートサービス(AWSサポート)は、サービスレベル別に4種類用意されている。 なお、いずれの形態であれ、日本語での問い合わせ対応が可能となっている。 **▼ベーシック** ・Management Console上で閲覧可能なヘルスチェックの表示のみ ・問い合わせ窓口：無し ・AWSのサービス利用料に包含されている **▼開発者** ・問い合わせ窓口：e-mailでの問い合わせ(平日9:00-18:00) ・初回応答時間：12時間 ・アーキテクチャーサポートレベル：個別要素のサポート **▼ビジネス** ・問い合わせ窓口：電話/チャット/e-mail(24時間365日) ・問い合わせ可能な担当者数：5名まで ・初回応答時間：1時間 ・アーキテクチャーサポートレベル：一般的なユースケースのガイダンス **▼エンタープライズ** ・問い合わせ窓口：電話/チャット/e-mail(24時間365日)、テクニカルアカウントマネージャ(TAM)への直接アクセス ・問い合わせ可能な担当者数：無制限 ・初回応答時間：15分 ・アーキテクチャーサポートレベル：アプリケーションのアーキテクチャ 【参考 URL】 http://aws.amazon.com/jp/premiumsupport/
5-4 運用監視	運用監視の対象/範囲(各レイヤ/システム(プロセス)/ネットワーク(パケット)等)、監視間隔	AWSでは監視機能やヘルスチェック機能を提供している。但し、OS以上のレイヤーに対しては個別に監視システムを構築する必要がある。 **▼CloudWatchで監視可能なメトリクス** ・EC2 - CPUUtilization - CPUCreditBalance / Usage - DiskReadOps / DiskWriteOps - DiskReadBytes / DiskWriteBytes - NetworkIn / NetworkOut - StatusCheckFailed - StatusCheckFailed_Instance - StatusCheckFailed_System ・EBS - VolumeIdleTime - VolumeQueueLength - VolumeReadBytes / VolumeWriteBytes - VolumeReadOps / VolumeWriteOps - VolumeTotalReadTime / VolumeTotalWriteTime ・RDS - BinLogDiskUsage - CPUUtilization - DatabaseConnections - DiskQueueDepth - FreeStorageSpace - FreeableMemory - NetworkReceiveThroughput - NetworkTransmitThroughput - Read / WriteIOPS - Read / WriteLatency - Read / WriteThroughput - SwapUsage ▼ELB ・Webサイトのヘルスチェックが可能 ※CloudWatch Logsを使用することでOS、アプリケーションやカスタムのログファイルを監視対象にすることができる。 （但し執筆時点では東京リージョン未対応のため、東京リージョンのインスタンスのログを対応リージョンに送り実装する等の工夫が必要） ※ディスク使用量やメモリ使用量といったメトリクスはEC2上のOSに依存するため、デフォルトでは提供されません。Windows版・Linux版のカスタムメトリクスを設定することで取得することが可能である。

	利用可能な運用監視ツール	AWSでも、オンプレミス環境と同様に、Zabbix/Hinemos/JP1などの主要な運用監視ツールを個別に導入・運用することが可能である。 **▼凡例: JP1ライセンスについて** JP1 Version 10の主要な製品が EC2上で利用できる ・JP1/Integrated Management ・JP1/Base ・JP1/Performance Management ・JP1/Automatic Operation ・JP1/Automatic Job Management System 3 ・JP1/File Transmission Server/FTP ・JP1/Cm2/Extensible SNMP Agent ・JP1/Cm2/SNMP System Observer - Agent for Process ほか ※ 対応OSは、Windows Server(R) 2003 R2, 2008, 2008 R2, 2012, Red Hat Enterprise Linux 5, 6となる。 【参考 URL】 http://www.hitachi.co.jp/Prod/comp/soft1/jp1/product/environment/cloud/index.html
5-5 リソース変更	仮想サーバー	AWSでは、仮想サーバーの起動・停止、スケールアウト/イン、スケールアップ/ダウンといったリソース変更が可能である。AWSでは予め大量にリソースを確保しているため、必要なリソース要求に対して遅延なく提供することが可能である。 **▼EC2の起動・停止** ・EC2は管理コンソール及びコマンドラインから起動・停止が可能 ※1. EC2停止の際は、一時ストレージとして利用可能なインスタンスストアの内容が消えるため、残しておきたいデータは永続ボリュームであるEBSに事前に移行しておくことを推奨する。 **▼EC2のスケールアップ/ダウン** ・EC2はインスタンスタイプを変更することで、性能の拡張・縮小が可能 ・インスタンスタイプの変更は、インスタンスの停止後、インスタンスのタイプを変更し、インスタンスを起動することで変更が可能 ※リザーブドインスタンスのインスタンスタイプを変更する場合、"予約済のインスタンスのユニット数"が一定となるように変更する必要がある。(例:smallインスタンス = 1ユニット、largeインスタンス = 4ユニット) **▼EC2のスケールアウト/イン** ・複数のEC2をロードバランサーサービス「ELB」の配下に並べることでスケールアウトの構成の構築が可能 ・モニタリングツール「CloudWatch」と自動スケールアウト機能「Auto Scaling」と組合せることで、負荷に応じて自動でスケールアウト/インするシステムの構築が可能 ※1. 数分間にトラフィックが数倍となるような急激なトラフィック変動はオートスケールで対処できないため、予め特定日時にスケールアウト/インするようにスケジューリングを考慮することを推奨する。 ※2. DBサーバーのスケールアウトはRDBサービス「RDS」のReadReplica機能などを活用することを推奨する。
	ストレージ	AWSでは、導入後もストレージ容量の変更や、IOPSの変更が可能である。 **▼EBSの容量拡張** ・EBSの容量拡張は、EBSスナップショットを取得・拡張し、EBSの付け替えとOSからの再認識を行うことで可能。 ※EBSの縮小はサポートされていないため、スモールスタートを意識したサイジングを推奨する。 **▼S3の容量拡張/縮小** ・S3は利用容量で課金され、容量の拡張/縮小を意識することなく利用が可能 **▼IOPSの変更** ・EBSのIOPS変更は、EBSスナップショットを取得・拡張し、ボリュームタイプの変更及びリザーブドIOPS値を変更後、EBSの付け替えとOSからの再認識を行うことで可能。
	ネットワーク	AWSでは、稼働中のセキュリティーグループやネットワークアクセスコントロールリスト(ACL)、ルートテーブルやサブネット、DHCPオプションといったネットワークのポリシー変更することが可能である。 **▼セキュリティーグループ/ネットワークアクセスコントロールリスト(ACL)/ルートテーブルの変更** ・セキュリティーグループ/ACL/ルートテーブルはいつでも変更が可能である。 ・適用するセキュリティーグループ/ACL/ルートテーブルの選択・解除はいつでも変更が可能である。 **▼サブネットの変更** ・適用するルートテーブルやACLの変更が可能である。 ・サブネットのアベイラビリティゾーンやCIディザスターリカバリー変更をするには、サブネットを作成し直す必要がある。 **▼インターネットゲートウェイの変更** ・VPCに適用するゲートウェイの適用・解除が可能である。 **▼DHCPオプションの変更** ・DHCPオプションの変更はできないため、新しいDHCPオプションセットを作成後、VPCに関連付けを行う必要がある。 ※一度作成したVPCのCIディザスターリカバリーのサイズ変更はできません。VPCのサイズが小さすぎて拡張に対応できない場合は、VPC内の全インスタンスを終了後、VPCの削除・作成が必要となる。
5-6 サーバーソフトウエア更新/パッチ適用	ソフトウエア更新/パッチ適用の実施方針/範囲	AWSで稼働する仮想サーバー(EC2)上で動作するOS/ミドルウエア/アプリケーションの各種ソフトウエア更新/パッチ適用をリモートで実施することが可能である。 ※1. RDSのデータベースソフトウエアへのパッチの適用はAWS側で自動的に実施される。数か月に一度、再起動を要するメンテナンスが発生する場合があるが、事前に希望のメンテナンス時間帯を指定しておくことが可能である。 ※2. AWSでは、仮想サーバー上のソフトウエア更新/パッチ適用以外にも、AWS管轄である仮想ホストやストレージ、ネットワーク機器などのサービス基盤へのパッチ適用を適宜実施しているため、稀にOSレベルの再起動やインスタンスレベルでの停止・開始の要求が通知される場合がある。

第6節　コンプライアンス要件

項目	要件	回答
6-1 拠点（DC）所在地域と仕様	クラウドサービス（IaaS、PaaS、SaaS）の稼働拠点（データセンター）の所在地域の国家・地方レベルでの指定	「 AWSは、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性を顧客に提供します。データとサーバーを配置する物理的なリージョンは、AWSのお客様が指定します。AWSは、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを 移動しないものとします。現在、AWS は、米国東部 – バージニア北部、米国西部 – 北カリフォルニアおよびオレゴン、GovCloud（米国）– オレゴン、南米 – サンパウロ、欧州 – アイルランド、アジアパシフィック – シンガポール、アジアパシフィック – 東京、アジアパシフィック – シドニーという9リージョンを提供しています。 」 *【参考 資料】Risk and Compliance White paper, P.19, データ管理　DG-02.4* *【参考 URL】http://aws.amazon.com/jp/about-aws/globalinfrastructure/*
	災害被害に関する立地条件	「 各アベイラビリティゾーンは、独立した障害ゾーンとして設計されています。つまり、アベイラビリティゾーンは、一般的な都市地域内で物理的に分離されており、洪水の影響が及ばないような場所にあります（洪水地域の分類はリージョンによって異なります）。個別の無停電電源装置（UPS）やオンサイトのバックアップ生成施設に加え、シングルポイントの障害の可能性を減らすために、別々の電力供給施設から異なる配管網を経由して、個別に電力供給を行っています。これらはすべて、冗長的に、複数の Tier-1 プロバイダに接続されています。 」 *【参考 資料】AWS Overview of Security Process White paper, P.7,事業継続性管理*
	災害被害に関する施設条件	「 各アベイラビリティゾーンは、独立した障害ゾーンとして設計されています。つまり、アベイラビリティゾーンは、一般的な都市地域内で物理的に分離されており、洪水の影響が及ばないような場所にあります（洪水地域の分類はリージョンによって異なります）。個別の無停電電源装置（UPS）やオンサイトのバックアップ生成施設に加え、シングルポイントの障害の可能性を減らすために、別々の電力供給施設から異なる配管網を経由して、個別に電力供給を行っています。これらはすべて、冗長的に、複数の Tier-1 プロバイダに接続されています。 」 *【参考 資料】AWS Overview of Security Process White paper, P.7,事業継続性管理* 「 Amazon のインフラストラクチャは高いレベルの可用性を備え、回復機能を持つ IT アーキテクチャを配備する機能を顧客に提供します。AWS のシステムは、顧客への影響を最小限に抑えながらシステムまたはハードウェア障害に耐えられるように設計されています。また、AWS におけるデータセンターの事業の継続性は、Amazon Infrastructure Group の指示に従って管理されます。 」 *【参考 資料】AWS Overview of Security Process White paper, P.7,事業継続性管理* 「 火災検出と鎮火 自動火災検出および鎮火装置が取り付けられ、リスクを軽減しています。この火災検出システムは、全データセンター環境、機械電気インフラ空間、冷却室および発電機設備室において、煙検出センサーを使用しています。これらのエリアは、充水型、二重連結予作動式、またはガス式スプリンクラーシステムによって守られています。 電力 データセンターの電力システムは、完全に冗長性をもち、運用に影響を与えることなく管理が可能となっています。1 日 24 時間体制で、年中無休で稼動しています。施設内で重要かつ不可欠な負荷に対応するために、電力障害時には無停電電源装置（UPS）がバックアップ電力を供給しています。データセンターは、発電機を使用して施設全体のバックアップ電力を供給しています。 天候と温度 サーバーその他のハードウェアの運用温度を一定に保つために、天候コントロールが必要です。これによって過熱を防ぎ、サーバー停止の可能性を減らすことができます。データセンターは、大気の状態を最適なレベルに保つように設定されています。作業員とシステムが、温度と湿度を適切なレベルになるよう監視してコントロールしています。 管理 AWSは、電気、機械、生命サポートシステムおよび設備をモニタリングし、問題が速やかに特定されるようにしています。予防的メンテナンスが実行され、設備を継続的な運用性が保たれています。 事故への対応 Amazonの事故管理チームは、業界標準の診断手順を採用しており、事業に影響を与えるイベント時に解決へと導きます。作業員スタッフが、24 時間 365 日体制で事故を検出し、影響と解決方法を管理します。 」 *3.AWS Overview of Security Process White paper, P.5,環境的セーフガード* 「 役員による全社的検査 Amazon の内部監査グループは、AWS サービスの復元プランを検査しました。このプランは、上級役員管理チームと取締役の監査委員会のメンバーによっても定期的に検査されています。 」 *4.AWS Overview of Security Process White paper, P.8,事業継続性管理*
	電源・空調の障害に関するファシリティ条件	「 Amazon のインフラストラクチャは高いレベルの可用性を備え、回復機能を持つ IT アーキテクチャを配備する機能を顧客に提供します。AWS のシステムは、顧客への影響を最小限に抑えながらシステムまたはハードウェア障害に耐えられるように設計されています。また、AWS におけるデータセンターの事業の継続性は、Amazon Infrastructure Group の指示に従って管理されます。 」 *【参考 資料】AWS Overview of Security Process White paper, P.7,事業継続性管理* 「 火災検出と鎮火 自動火災検出および鎮火装置が取り付けられ、リスクを軽減しています。この火災検出システムは、全データセンター環境、機械電気インフラ空間、冷却室および発電機設備室において、煙検出センサーを使用しています。これらのエリアは、充水型、二重連結予作動式、またはガス式スプリンクラーシステムによって守られています。 電力 データセンターの電力システムは、完全に冗長性をもち、運用に影響を与えることなく管理が可能となっています。1 日 24 時間体制で、年中無休で稼動しています。施設内で重要かつ不可欠な負荷に対応するために、電力障害時には無停電電源装置（UPS）がバックアップ電力を供給しています。データセンターは、発電機を使用して施設全体のバックアップ電力を供給しています。 天候と温度 サーバーその他のハードウェアの運用温度を一定に保つために、天候コントロールが必要です。これによって過熱を防ぎ、サーバー停止の可能性を減らすことができます。データセンターは、大気の状態を最適なレベルに保つように設定されています。作業員とシステムが、温度と湿度を適切なレベルになるよう監視してコントロールしています。 管理 AWSは、電気、機械、生命サポートシステムおよび設備をモニタリングし、問題が速やかに特定されるようにしています。予防的メンテナンスが実行され、設備を継続的な運用性が保たれています。 」 *【参考 資料】AWS Overview of Security Process White paper, P.5,環境的セーフガード* 「 事故への対応 Amazonの事故管理チームは、業界標準の診断手順を採用しており、事業に影響を与えるイベント時に解決へと導きます。作業員スタッフが、24 時間 365 日体制で事故を検出し、影響と解決方法を管理します。 役員による全社的検査 Amazon の内部監査グループは、AWS サービスの復元プランを検査しました。このプランは、上級役員管理チームと取締役の監査委員会のメンバーによっても定期的に検査されています。 」 *【参考 資料】AWS Overview of Security Process White paper, P.7,事業継続性管理*

	不法侵入や妨害破壊行為などに関する物理セキュリティ条件	「 AWSは大規模データセンターの設計、構築、運用において、長年の経験を有しています。この経験は、AWSプラットフォームとインフラストラクチャに活かされています。AWS のデータセンターは、外部からはそれとはわからないようになっています。ビデオ監視カメラ、最新鋭の侵入検出システム、その他エレクトロニクスを使った手段を用いて、専門のセキュリティスタッフが、建物の入口とその周辺両方において、物理的アクセスを厳密に管理しています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行います。 AWSは、必要とする正規の手続きを有する従業員や業者に対してのみ特権を与え、データセンターへのアクセスや情報を提供しています。従業員がこれらの特権を必要とする作業を完了したら、たとえかれらが引き続き Amazon または Amazon Web Services の従業員であったとしても、そのアクセス権は速やかに取り消されます。AWS従業員によるデータセンターへのすべての物理的アクセスは記録され、定期的に監査されます。 」 *1.AWS Overview of Security Process White paper, P.5,物理的セキュリティ*
	運用体制に関する条件	「 **設定管理** 既存のAWSインフラストラクチャに対する緊急、非定期的、その他の設定の変更は、こうしたシステムで適用される業界基準に従って、認定、記録、テスト、承認を経て、文書化されます。AWS インフラストラクチャを更新するにあたり、顧客とその顧客のサービス使用への影響は最小限に抑えられます。サービスが悪影響を受ける可能性がある場合、AWS は E メールまたは AWS Service Health Dashboard（http://status.aws.amazon.com/）を通じて顧客に通知します。 」 *【参考 資料】AWS Overview of Security Process White paper,P6, 設定管理* 「 **モニタリング** AWSは、自動モニタリングシステムを活用して、ハイレベルなサービスパフォーマンスと可用性を提供します。内部的、外部的両方の使用において、様々なオンラインツールを用いた積極的モニタリングが可能です。AWS内のシステムには膨大な装置が備わっており、重要な運用上の計測値をモニタリングしています。運用上の重要計測値が早期警戒閾値を超える場合に運用管理担当者に通知されるよう、アラームが設定されています。オンコールスケジュールが採用されているので、担当者が運用上の問題にいつでも対応できます。ポケットベルシステムがサポートされ、アラームが迅速かつ確実に運用担当者に届きます。障害や問題の処理時には、運用担当者を支援して情報を提供するための文書が保持されます。問題の解決のために協力体制が必要な場合は、情報伝達と記録機能をサポートする会議システムが使用されます。協力体制を必要とする運用上の問題の処理にあたっては、訓練を受けた通話リーダーが、コミュニケーションと進捗を支援します。深刻な運用上の問題が発生した後には、外部的な影響の有無に関わらず、事後分析会議が開かれます。そしてエラーの原因（COE）に関する文書が起草され、根本的な原因が捕捉されて、今後のために予防措置が取られるようにします。予防措置の実施は、週に一度開かれる運用会議において追跡されます。 」 *【参考 資料】AWS Overview of Security Process White paper, P.4,モニタリング* 「 <u>事故への対応</u> Amazonの事故管理チームは、業界標準の診断手順を採用しており、事業に影響を与えるイベント時に解決へと導きます。作業員スタッフが、24 時間 365 日体制で事故を検出し、影響と解決方法を管理します。 」 「 **リスク管理** AWSマネジメントは、リスクを緩和または管理するためのリスク特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、戦略的事業計画を再評価します。このプロセスでは、マネジメントがその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。 」 *【参考 資料】Risk and Compliance White paper, P.6, リスク管理*
6-2 データ所在の把握/特定（国/地域）	・クラウドサービスが取り扱う企業・機関の機密情報やセンシティブ情報の保持場所についての把握 ・情報が事前に指定した（国家・地方などの）地域の国内法が及ぶ範囲限定であることについて	6-1 クラウドサービス（IaaS、PaaS、SaaS）の稼働拠点（データセンター）を参照
6-3 法令/業界規制/社内基準/標準化	・刑法、著作権法、不正アクセス禁止法、個人情報保護法等各種法令/規制への対応 ・IPAでのガイドラインで取り上げられている項目について ・公的認証機関等のガイドラインまたは認定基準の準拠	「 固有の統制の定義。AWSのお客様は、AWSが管理する主な統制を指定できます。主な統制はお客様の統制環境にとって不可欠であり、年次の会計監査などのコンプライアンス要件に準拠するには、その主な統制の運用効率について外部組織による証明が必要です。そのために、AWS は Service Organization Controls 1（SOC 1）Type II レポートで幅広く詳細な IT 統制を公開しています。 」 *【参考 資料】Risk and Compliance White paper, P.4,AWS 統制の評価と統合* 「 一般的な統制基準の準拠。AWS のお客様がさらなる統制目標を満たす必要がある場合は、AWS の業界認定の評価を行うことも可能です。AWSは幅広く包括的なセキュリティ基準に準拠し、安全な環境を維持するためのベストプラクティスに従っており、ISO 27001 認定を取得しています。AWS はクレジットカード情報を処理する会社にとって重要な統制に準拠しており、PCI Data Security Standard（PCI DSS）の認定を取得しています。AWSは米国政府機関から要求される幅広く詳細な統制に準拠しており、FISMA 基準に準拠しています。このような一般的な基準に準拠しているので、お客様は所定の統制およびセキュリティプロセスの包括的な特性について詳細な情報を得ることができます。また、コンプライアンスを管理するときに、それらの基準の準拠について考慮できます。 」 *【参考 資料】Risk and Compliance White paper, P.4,AWS 統制の評価と統合* 「 AWS統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWSのコンプライアンスおよびセキュリティチームは、Control Objectives for Information and related Technology（COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを規定しました。また、ISO 27002 統制、PCI DSS、およびアメリカ国立標準技術研究所（National Institute of Standards and Technology/NIST ）出版物 800-53 Rev 3（Recommended Security Controls for Federal Information Systems）に基づいて、ISO 27001に認定可能なフレームワークを効果的に統合しました。AWSは、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実行します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。 」 *【参考 資料】Risk and Compliance White paper, P.5, リスク管理* 「 AWSは外部の認定機関および独立監査人と協力し、AWSが構築および運用しているポリシー、プロセス、および統制に関して多数の情報をお客様に提供しています。 」 *【参考 資料】Risk and Compliance White paper, P.7,AWS の認定とサードパーティによる証明*
	個人情報保護法の遵守	「 お客様の代理で AWS が保存しているすべてのデータは、強力なテナントの隔離セキュリティと統制機能で保護されています。お客様が自身のデータの統制と所有権を有しているので、データの暗号化を選択するのはお客様の責任です。AWS では、S3、EBS、SimpleDB、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。VPC セッションも暗号化されます。また、Amazon S3 は、お客様向けのオプションとしてサーバー側の暗号化も提供しています。詳細については、「AWS Risk and Compliance Whitepaper」（http://aws.amazon.com/security）を参照してください。 」 *【参考 資料】Risk and Compliance White paper, P.18, コンプライアンス 情報システムの規制,マッピング ,CO-05.1* ・個人情報保護法の遵守については、第3者機関の認証であるSOC2により保証される。 ・SOC2は、サービスのセキュリティ性、可用性、処理の整合性、機密性、個人情報保護の5原則を基準に、合計127の領域において、提供するサービスの業務プロセスと統制環境が基準を満たしているか監査を通じて検証し、該当基準を満たした場合に付与される。 *【参考 資料】Risk and Compliance White paper, P.17 独立監査、CO-02.1*

	ISMS（JIS Q 27001:2006、ISM/IEC 27001:2005）対応状況	「 **固有の統制の定義。**AWSのお客様は、AWSが管理する主な統制を指定できます。主な統制はお客様の統制環境にとって不可欠であり、年次の会計監査などのコンプライアンス要件に準拠するには、その主な統制の運用効率について外部組織による証明が必要です。そのために、AWS は Service Organization Controls 1（SOC 1）Type II レポートで幅広く詳細な IT 統制を公開しています。 」 *【参考 資料】Risk and Compliance White paper, P.4,AWS 統制の評価と統合* 「 **一般的な統制基準の準拠。**AWS のお客様がさらなる統制目標を満たす必要がある場合は、AWS の業界認定の評価を行うことも可能です。AWSは幅広く包括的なセキュリティ基準に準拠し、安全な環境を維持するためのベストプラクティスに従っており、ISO 27001 認定を取得しています。AWS はクレジットカード情報を処理する会社にとって重要な統制に準拠しており、PCI Data Security Standard（PCI DSS）の認定を取得しています。AWS は米国政府機関から要求される幅広く詳細な統制に準拠しており、FISMA 基準に準拠しています。このような一般的な基準に準拠しているので、お客様は所定の統制およびセキュリティプロセスの包括的な特性について詳細な情報を得ることができます。また、コンプライアンスを管理するときに、それらの基準の準拠について考慮できます。 」 *【参考 資料】Risk and Compliance White paper, P.4,AWS 統制の評価と統合* 「 AWS統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWSのコンプライアンスおよびセキュリティチームは、Control Objectives for Information and related Technology（COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを規定しました。また、ISO 27002 統制、PCI DSS、およびアメリカ国立標準技術研究所（National Institute of Standards and Technology/NIST ）出版物 800-53 Rev 3（Recommended Security Controls for Federal Information Systems）に基づいて、ISO 27001に認定可能なフレームワークを効果的に統合しました。AWSは、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実行します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。 」 *【参考 資料】Risk and Compliance White paper, P.5, リスク管理*
	物理ストレージの破棄方法	「 ストレージデバイスの廃棄 ・AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は、DoD 5220.22-M（「National Industrial Security Program Operating Manual（国立産業セキュリティプログラム作業マニュアル）」）または NIST 800-88（「Guidelines for Media Sanitization（メディア衛生のためのガイドライン）」）に詳細が記載されている技術を用いて、廃棄プロセスの一環としてデータを破棄します。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。 」 *【参考 資料】Risk and Compliance White paper, P.12, 主なコンプライアンスの問題と AWS*
6-4 監査基準対応	立ち入り検査などの監査対応について	・AWS のデータセンターでは複数のお客様をホストしており、幅広いお客様を第三者の物理的アクセスにさらすことになるため、お客様によるデータセンター訪問を許可していません。このようなお客様のニーズを満たすために、SOC 1 Type II レポート（SSAE 16）の一環として、独立し、資格を持つ監査人が統制の有無と運用を検証しています。この広く受け入れられているサードパーティによる検証によって、お客様は実行されている統制の効果について独立した観点を得ることができます。AWS と機密保持契約を結んで いるAWSのお客様は、SOC 1 Type II レポートのコピーを要求できます。 データセンターの物理セキュリティの独立した見直しは、ISO 27001監査、PCI評価、ITAR監査、およびFISMAテストプログラムにも含まれています。 ・SSAE 16 (SOC1) 監査により、データとネットワークセキュリティ、論理的セキュリティ、バックアップと復旧の手続き、システムの可用性、アプリケーション開発、顧客の認証を含む管理体制について第3者による監査が行われたことを証明することができる。 *【参考 資料】Risk and Compliance White paper, P.12, 主なコンプライアンスの問題と AWS*
	利用者からの要請に応じて、監査対応に必要な各種情報の収集が可能なこと。	・インスタンス上に残る各種ログと、サービスが提供するログをシステム管理者が収集可能。 ・CloudTrailサービス（2013年11月より提供）により操作履歴の記録が可能。 ・SSAE 16 (SOC1) 監査により、データとネットワークセキュリティ、論理的セキュリティ、バックアップと復旧の手続き、システムの可用性、アプリケーション開発、顧客の認証を含む管理体制について第3者による監査が行われたことを証明することができる。 *【参考 URL】http://aws.amazon.com/jp/console/* *【参考 資料】Risk and Compliance White paper, P.17 独立監査、CO-02.1* 「 AWSの認定とサードパーティによる証明 AWSの製品およびサービス一覧（リージョン別）についての最新情報は下記のURLを参照ください。 *【参考 URL】http://aws.amazon.com/jp/about-aws/globalinfrastructure/* *【参考 URL】http://aws.amazon.com/jp/about-aws/globalinfrastructure/regional-product-services/* 」
	脆弱性のテスト、ネットワーク侵入テストを定期的に実行しているか	AWS インフラストラクチャの健全性と可視性を確認するために、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンする（お客様のインスタンスはこのスキャンの対象外）。判明した脆弱性があれば、修正するために適切な関係者に通知する。さらに、脆弱性に対する外部からの脅威の査定が、独立系のセキュリティ会社によって定期的に実行される。これらの査定に起因する発見や推奨事項は、分類整理されて AWS 上層部に報告される。 *【参考 資料】Risk and Compliance White paper, P.6 リスク管理*
	内部監査/外部監査を定期的に実施しているか	監査の定期的な実施などのAWS統制環境は、通常の内部的 および外部的リスク評価によって規定されている。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしている。外部の脆弱性脅威評価を 実行するために、独立したセキュリティ会社と定期的に契約している。 *【参考 資料】Risk and Compliance White paper, P.18 独立監査、CO-02.5* *【参考 資料】Risk and Compliance White paper, P.18 サードパーティ監査、CO-03.2*
	テナントに対して、独立した脆弱性評価の実行可否	独立した脆弱性評価の実行は可能。スキャンを実施する許可をリクエストできる。このようなスキャンについて事前に承認を受けるには、AWS 脆弱性／侵入テストリクエスト フォームを使用して申請を行う。 *【参考 資料】Risk and Compliance White paper, P.18 サードパーティ監査、CO-03.2*
6-5 その他の要件	AWS公開情報にはない情報	コンプライアンスに関する要件は、リーガルアドバイスに関わるケースバイケースの問題となることが多いためパートナーにご相談ください。
6-6 コンプライアンス情報	コンプライアンス関連文書	AWSコンプライアンスに関する最新の情報に関しては下記を参照。 ・AWS セキュリティセンター,AmazonWebService http://aws.amazon.com/jp/security/ ・AWS コンプライアンス,AmazonWebService http://aws.amazon.com/jp/compliance/ ・ホワイトペーパー（リスクとコンプライアンス）,2012年7月,AmazonWebService Risk and Compliance White paper

第7節　ベンダー要件

項目	要件	回答
7-1 グローバル対応/標準化	グローバルな拠点で均一なサービスの利用	・全世界共通のコンソールサービスを展開している。 ・リージョンごとにサービスの種類で差異はあるが、サービス仕様は共通化している。 ・AWSの製品およびサービス一覧（リージョン別）についての最新情報は下記のURLを参照。 *【参考 URL】http://aws.amazon.com/jp/about-aws/globalinfrastructure/* *【参考 URL】http://aws.amazon.com/jp/about-aws/globalinfrastructure/regional-product-services/*
7-2 事業継続	災害発生時、パンデミック発生時の事業継続のための対応手順、体制	・サービスを提供するプロセス（運用や体制など）について、プロセス基準書を定義し、障害災害対応手順書や体制を整備し、訓練計画書に沿って、定期的な訓練を実施している。 「 **リスク管理** ・AWSマネジメントは、リスクを緩和または管理するためのリスク特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、戦略的事業計画を再評価します。このプロセスでは、マネジメントがその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。 」 *【参考 資料】Risk and Compliance White paper, P.6, リスク管理* 「 管理 AWSは、電気、機械、生命サポートシステムおよび設備をモニタリングし、問題が速やかに特定されるようにしています。予防的メンテナンスが実行され、設備を継続的な運用性が保たれています。 事故への対応：Amazonの事故管理チームは、業界標準の診断手順を採用しており、事業に影響を与えるイベント時に解決へと導きます。作業員スタッフが、24 時間 365 日体制で事故を検出し、影響と解決方法を管理します。 」 *【参考 資料】AWS Overview of Security Process White paper, P.5,環境的セーフガード* 「 事故への対応 ・Amazonの事故管理チームは、業界標準の診断手順を採用しており、事業に影響を与えるイベント時に解決へと導きます。作業員スタッフが、24 時間 365 日体制で事故を検出し、影響と解決方法を管理します。 役員による全社的検査 Amazon の内部監査グループは、AWS サービスの復元プランを検査しました。このプランは、上級役員管理チームと取締役の監査委員会のメンバーによっても定期的に検査されています。 」

本付録で使用されている登録商標または商標を以下に列挙いたします。ただしここに含まれないものも特定の法人または個人の登録商標または商標である可能性があります。
・Opteronは、Advanced Micro Devices, Inc. （AMD）または子会社の米国およびその他の国における商標です。
・Xeonは、アメリカ合衆国および / またはその他の国における Intel Corporation の商標です。
・Linuxは、Linus Torvalds氏の日本およびその他の国における登録商標または商標です。
・Windowsの正式名称はMicrosoft Windows Operating Systemです。
・Red Hat Enterprise Linuxは、米国またはその他の国における Red Hat, Inc. の登録商標です。
・NovellおよびSUSEは、米国およびその他の国におけるNovell,Inc. の登録商標です。
・Ubuntuは、Canonical Ltd.の登録商標です。
・CentOSは、CentOS ltd.の商標または登録商標です。
・Debianは、Software in the Public Interest, Inc.の登録商標です。
・Microsoft、Windows、Windows Server、SQL Server、Internet Information Server（IIS）、Microsoft .NET Framework SDK(.Net)、Exchange Server、SharePoint Server、Lync Server、System Center Server、Dynamics CRM、Dynamics AX、Hyper-Vは、米国Microsoft Corporationの米国およびその他の国における登録
・MySQLは、MySQL AB社の登録商標です。
・PostgreSQLはPostgreSQLの米国およびその他の国における商標 です。
・Oracle、Oracle Database、Java、Oracle WebLogic Serverは、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における商標または登録商標です。
・Node.js は Joyent, Inc の商標です。
・Pythonは、Python Software Foundationの登録商標または商標です。
・Android は、Google Inc.の商標または登録商標です。
・IOSはCiscoの米国およびその他の国の登録商標であり、Apple Inc.がライセンスに基づき使用しています。
・HULFTは、株式会社セゾン情報システムズの登録商標 または商標です。
・DataSpiderは、株式会社アプレッソの商標です。
・VMwareは、米国またはその他の国における VMware, Inc. の登録商標または商標です。
・Zabbixはラトビア共和国にあるZabbix SIAの商標です。
・Hinemosは、 株式会社NTTデータの登録商標です。
・JP1、JP1/Integrated Management、JP1/Base、JP1/Performance Management、JP1/Automatic Operation、JP1/Automatic Job Management System 3、JP1/File Transmission Server/FTP、JP1/Cm2/Extensible SNMP Agent、JP1/Cm2/SNMP System Observer - Agent for Processは、株式会社日立製作所の日本における商品名称(商標または登録商標)です。
・Amazon Web Services、AWS、Amazon EC2、Amazon EBS、Amazon S3、Amazon VPC、AWS Direct Connect、Auto Scaling、Amazon Glacier、AWS Storage Gateway、Amazon RDS、Amazon ELB、Amazon Route53、Amazon Dynamo DB、Amazon Redshift、AWS Data Pipeline、Amazon EMR、Amazon CloudFront、Amazon ElastiCache、Amazon SES、Amazon SNS、Amazon SQS、Amazon SWF、Amazon Cloud Search、Amazon Elastic Transcoder、Amazon Elastic Beanstalk、AWS CloudFormation、AWS OpsWorks、AWS IAM、AWS Management Console、Amazon CloudWatch、Amazon CloudTrail、Amazon SimpleDB、AWS SDKは、米国その他の諸国における、Amazon.com, Inc.またはその関連会社の商標です。
・その他記載されている会社名、製品名などの固有名詞は、それぞれの会社の商標または登録商標です。
・記載されているシステム名、製品名等には、必ずしも商標表示（(R)、TM ）を付記していません。
・本付録では、説明等の便宜のために製品名、会社名等を掲載する場合がありますが、それらの商標権の侵害を行う意志や目的はありません。
※本書に記載された内容に関して執筆者一同はいかなる保証を行うものではなく、またこの文書を明示的または暗黙的に利用した結果について責任を負うものではありません。