『金融機関等コンピュータシステムの安全対策基準・解説書（第8版追補改訂）』（運108～113）

***Amazon Web Services* の情報 2017年5月**

本文書は、『金融機関等コンピュータシステムの安全対策基準・解説書（第8版追補改訂）』で追加された基準に対するAWSの情報です。
『金融機関等コンピュータシステムの安全対策基準・解説書（第8版追補改訂）』の全体に関する情報については、『金融機関等コンピュータシステムの安全対策基準・解説書（第8版）』に対する情報とあわせてご確認ください。
（URL: https://aws.amazon.com/jp/compliance/fisc/）

基準大項目	中項目	項番	小項目	基準項目の目的　内容説明　具体例等の解説	AWSの情報
運用基準	クラウドサービスの利用	運108	クラウドサービスの利用を行う場合は、事前に利用目的や範囲等を明確にするとともに、事業者選定の手続きを明確にすること。	1.　クラウド事業者を選定するにあたっては、事前に目的や範囲等を明確にしたうえで、選定手続きを明確にすることが必要である。 2.　明確にすべきクラウドサービスの利用に関する事項としては以下の例がある。	AWS利用者のシステム、サービス、リスク、コスト等、一般的なITシステムに関する考慮事項についての検討やAWSサービス利用にあたってのAWS利用者の責任範囲は、AWSサービスの選定や利用方法、既存のIT環境への該当サービスの統合方法、該当リージョンにおいて適用される法律および規制等、諸条件によって異なります。したがって、利用に際してのリージョンの選択、サービスの選択やその構成について注意深く検討いただく必要があります。 クラウドサービスの利用目的や範囲等の明確化およびクラウド事業者の選定にかかる手続きの明確化についても、AWS利用者の実施事項となります。
				3.　クラウド事業者を客観的に評価すること。 クラウドサービスを利用する業務に求められる可用性・機密性等の観点及び自社の経営の視点から、リスクを分析・認識し、当該業務に求められるリスク管理レベルを検討のうえ、その実現が可能なクラウド事業者を選定すること。その際、クラウド事業者の資質・業務遂行能力に関する情報や、クラウド事業者の内部統制やリスク管理に関する状況等をもとに評価を行うことが必要である(注)。評価にあたっては、クラウド事業者によって契約前の情報開示に消極的なケースもあるが、必要に応じ機密保持契約を事前に締結したうえで開示を求めることが望ましい。 (注) 資源共有型であるパブリッククラウドの場合、クラウド事業者によっては、標準的な契約・SLA等の内容に関し個社からの変更要求に応じないことも想定されるため、各金融機関が特に重要であると判断した事項については、こうした変更要求の交渉が可能であるかを事前に確認しておくことが必要である。 ただし、金融機関等において業務の特性を十分検討した上で、委託する業務の重要度が高くないと判断し得る場合は、クラウド事業者の公開情報や、業界における評判や実績等による客観的な評価を行うことも可能である。 評価する事項としては、以下のような例がある。	AWSは、インターネット上のウェブサイト、ホワイトペーパー、レポート、認定、その他サードパーティによる証明を通じて、当社のIT統制環境に関する幅広い情報をお客様にご提供しています。本文書は、お客様が使用するAWSサービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様にご理解いただくことをお手伝いするためのものです。この情報はまた、お客様の拡張されたIT環境内の統制が効果的に機能しているかどうかを明らかにし、検証するのにも有用です。 AWS導入事例： https://aws.amazon.com/jp/solutions/case-studies/all/ AWS ウェブサイト： https://aws.amazon.com/ AWSアナリストレポート： https://aws.amazon.com/jp/resources/analyst-reports/ AWSコンプライアンス・ウェブサイト： https://aws.amazon.com/jp/compliance/ AWSセキュリティ・ウェブサイト： https://aws.amazon.com/jp/security/ 各種認定やサードパーティによる保証： https://aws.amazon.com/jp/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/ AWS カスタマーアグリーメント： https://aws.amazon.com/jp/agreement/ （参考）サービスレベルアグリーメント（一部）： https://aws.amazon.com/jp/ec2/sla/ https://aws.amazon.com/jp/route53/sla/ https://aws.amazon.com/jp/rds/sla/ https://aws.amazon.com/jp/cloudfront/sla/ https://aws.amazon.com/jp/s3/sla/

基準大項目	中項目	項番	小項目	基準項目の目的　内容説明　具体例等の解説	AWSの情報
				4.　紛争が生じた際にどの国の法律が適用されるのか、また、現地の公権力による捜査目的で、データが差し押えられるといった場合に、業務の継続性に影響がないかといった点には十分に配慮する必要がある。特に、重要業務を委ねる場合には、データが分散格納されている場合を含めて、データの所在を把握することが重要になる。 高い可用性が求められる業務処理を行ったり、機密性の高い顧客情報の処理・蓄積・保管を行ったりする場合には、当該クラウドサービスに適用される法令が特定できる範囲で所在地域(国、州等)を把握する必要がある。 勘定系システム等の極めて高い可用性・信頼性が求められるシステムについては、データセンターの立地状況等を見極める観点から、詳細な所在地まで把握する必要がある。 インシデント発生時にデータセンターへの立入が必要になる場合や立入監査を行う際には、具体的な所在地を把握する必要がある。 ただし、委託する業務の重要度に応じて、データの所在について把握する必要性や把握の詳細度に差異が生じることはあり得る。したがって、金融機関等において業務の特性を十分検討した上で、委託する業務の重要度が高くないと判断し得る場合には、データの所在地に関する情報の把握について省略することも可能である。	AWS利用者のシステム、サービス、リスク、コスト等、一般的なITシステムに関する考慮事項についての検討やAWSサービス利用にあたってのAWS利用者の責任範囲は、AWSサービスの選定や利用方法、既存のIT環境への該当サービスの統合方法、該当リージョンにおいて適用される法律および規制等、諸条件によって異なります。したがって、利用に際してのリージョンの選択、サービスの選択は注意深く検討いただく必要があります。 準拠法および裁判所については、「AWS カスタマーアグリーメント」をご参照ください。 https://aws.amazon.com/jp/agreement/ AWSは、日本の利用者に対して、リクエストに応じて日本法準拠および東京地裁への変更を提示しています。
				5.　クラウド事業者との間で係争が生じた場合の準拠法やこれを取り扱う裁判所に関する取決めが他国である場合に、クラウド事業者の選定にあたって評価すべきリスクとしては、以下のようなものがある。	AWS利用者のシステム、サービス、リスク、コスト等、一般的なITシステムに関する考慮事項についての検討やAWSサービス利用にあたってのAWS利用者の責任範囲は、AWSサービスの選定や利用方法、既存のIT環境への該当サービスの統合方法、該当リージョンにおいて適用される法律および規制等、諸条件によって異なります。したがって、利用に際してのリージョンの選択、サービスの選択やその構成について注意深く検討いただく必要があります。 準拠法および裁判所については、「AWS カスタマーアグリーメント」をご参照ください。 https://aws.amazon.com/jp/agreement/ AWSは、日本の利用者に対して、リクエストに応じて日本法準拠および東京地裁への変更を提示しています。
				6.　クラウド事業者の決定には、責任者の承認を得ることが必要である。	AWS利用者のシステム、サービス、リスク、コスト等、一般的なITシステムに関する考慮事項についての検討やAWSサービス利用にあたってのAWS利用者の責任範囲は、AWSサービスの選定や利用方法、既存のIT環境への該当サービスの統合方法、該当リージョンにおいて適用される法律および規制等、諸条件によって異なります。したがって、利用に際してのリージョンの選択、サービスの選択やその構成について注意深く検討いただく必要があります。 クラウド事業者の決定にかかる承認手続きはAWS利用者の実施事項となります。
				7.　クラウド事業者が提供するサービス等の導入に際しては、必要に応じて【運72、運73】も参照のこと。	AWS利用に際しての【運72】、【運73】の参照要否の判断については、AWS利用者における実施事項となります。

基準大項目	中項目	項番	小項目	基準項目の目的　内容説明　具体例等の解説	AWSの情報
		運109	クラウド事業者と安全対策に関する項目を盛り込んだ契約を締結すること。	1.　クラウドサービスを利用する業務の種類や範囲に応じて、クラウド事業者と契約を締結すること。 契約時に考慮すべき事項については、以下のような例がある。なお、クラウド事業者との契約やSLAの締結、SLO(Service Level Objective、サービス事業者がサービスの品質について目標を定めたもの)の確認にあたっては、以下の例の他に、各金融機関が委託する業務のプロファイルに応じて必要と判断する事項を追加、変更することも考えられる。さらに、必要に応じて「サービスを利用するための契約」とは別に「リスク管理に関する契約」を締結することも考えられる。	AWS利用者のシステム、サービス、リスク、コスト等、一般的なITシステムに関する考慮事項についての検討やAWSサービス利用にあたってのAWS利用者の責任範囲は、AWSサービスの選定や利用方法、既存のIT環境への該当サービスの統合方法、該当リージョンにおいて適用される法律および規制等、諸条件によって異なります。したがって、利用に際してのリージョンの選択、サービスの選択やその構成について注意深く検討いただく必要があります。 「サービスアグリーメント」等の契約内容に関する評価は、AWS利用者における実施事項となります。 AWSアーキテクチャセンターでは、AWSクラウド環境上でスケーラブルで信頼性の高いアプリケーションの構築に必要なガイダンスやアプリケーションアーキテクチャのベストプラクティスを提供しています。AWSのプラットフォーム、そのサービスや機能の理解に役立ち、AWSインフラストラクチャで実行されるシステムの設計と実装のためのアーキテクチャに関するガイダンスも提供しています。構築したシステム全体の信頼性、サービスレベル・オブジェクティブ、サービスレベル・アグリーメントは、サービスの利用方法や、システム設計・構成によって異なります。 AWSアーキテクチャセンター： https://aws.amazon.com/jp/architecture/
				2.　SLAの締結やSLOの確認により、サービスレベル(注)について合意することが望ましい。 SLA及びSLOに記載すべき指標には以下のような例がある。 (注) クラウド事業者との契約の中にはSLAが含まれるのが通例であるが、多くの標準的なSLAでは、基準となる月間稼働率などを定めたうえで、実際の稼働率が基準を下回った場合にサービスの利用料を減額するといった内容にとどまっている。そのため、例えば、勘定系システムのオンライン処理など高い稼働率が求められる場合では、こうした標準的なSLAによる契約締結では不十分な可能性がある。 クラウド事業者の顧客は金融機関をはじめ、さまざまな業種にわたる。その中で各顧客企業との間で個別の内容の契約を準備するのは効率的ではないとの考えから、クラウド事業者はSLAを個別に締結することに対し消極的な場合もある。一方で、金融機関が特に重要な業務を委託する場合においては、その社会的な重要性に鑑み、相応の高いサービスレベルが求められる。	個別のAWSサービスのサービスレベルアグリーメントは下記を参照ください。サービスレベルアグリーメントは、AWS利用に関する契約の一部であり、サービスのレベルを正式に定義しています。AWSは、AWSのサービスレベルアグリーメント(SLA)に従い、機能停止によって発生する可能性がある損失について、お客様に賠償を提供しています。 AWS カスタマーアグリーメント： https://aws.amazon.com/jp/agreement/ AWSサービスレベルアグリーメント： https://aws.amazon.com/jp/ec2/sla/ https://aws.amazon.com/jp/route53/sla/ https://aws.amazon.com/jp/rds/sla/ https://aws.amazon.com/jp/cloudfront/sla/ https://aws.amazon.com/jp/s3/sla/ 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、主要なオペレーションメトリックをモニタリングしています。重要計測値が早期警戒しきい値を超える場合に運用管理担当者に自動的に通知されるよう、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。
				3.　委託する業務の重要度に応じて、契約やSLAに盛り込まれる内容や基準値が異なるほか、内容自体の必要性も変わり得る。したがって、金融機関等において業務の特性を十分検討した上で、委託する業務の重要度が高くないと判断し得る場合には、必ずしも上記1.～2.のすべてを必要とせず、クラウド事業者が提示する標準的なSLAを締結することや一般的な契約の締結のみを行い、SLAの締結を省略することも可能である。	

基準大項目	中項目	項番	小項目	基準項目の目的　内容説明　具体例等の解説	AWSの情報
				4.　サービスレベル合意の違反のほか、クラウド事業者や金融機関の方針変更によってクラウド事業者との契約の続行が困難になるような場合でも、業務の継続を可能とするため、事前に代替のクラウドサービスや一般のアウトソーシングに移行する、もしくはオンプレミスの環境に移行することができるような対策を講ずることが望ましい。 例えば、以下のような例がある。	AWS利用者はデータの統制と所有権を保持します。AWSでは、必要に応じてAWS利用者はデータをAWSのストレージサービスへにインポート・エクスポートすることが可能です。 Amazon S3用AWS Import/Exportサービスでは、転送用のポータブル記憶装置を使用して、AWS内外への大容量データの転送を高速化することも可能です。AWSでは、お客様がご自分のテープバックアップサービスプロバイダを使用してテープへのバックアップを実行することも可能ですが、AWSではテープへのバックアップサービスの提供は実施しておりません。 また、AWS利用者はAmazon Machine Images(AMI)をエクスポートして、施設内または別のサービスプロバイダーで使用可能です。(ただし、該当ソフトウェア・OSのライセンス制限に従います。) Amazon Machine Images (AMI)： http://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/AMIs.html AWSのご利用停止に備えた代替策の検討・実施については、AWS利用者における実施事項となります。また、契約解除後のAWS利用者のデータ取り出し等に関するAWSによる支援については、「AWSカスタマーアグリーメント」をご参照ください。 AWSカスタマーアグリーメント： https://aws.amazon.com/jp/agreement/
		運110	クラウドサービス利用にあたって、データ漏洩防止策を講ずること。	1.　クラウド事業者にデータ管理を委託する場合、漏洩防止策を講ずることが必要である。 暗号化を含むデータ保護については、以下のような例がある。【技28】【技29】 ただし、暗号化やトークン化等の代替策は、顧客データ等の重要なデータを保全するための管理策であり、金融機関等において、情報の機密性や業務におけるリスクプロファイルにより重要なデータでないと判断し得る場合は、暗号化やトークン化等の管理策を省略することも可能である。	AWSでは、Amazon S3、Amazon EBS、Amazon SimpleDB、Amazon 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へのIPSecトンネルも暗号化されます。 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。 お客様は、サードパーティの暗号化テクノロジを使用することもできます。 AWSの暗号化関連プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP へのAWSの継続的な準拠のために、第三者の独立監査人によって確認されます。また、AWSは、インターネット上のウェブサイト、ホワイトペーパー、認定、その他サードパーティによる証明を通じて、AWSの暗号化関連サービス、暗号化キーの作成と管理に関する情報をお客様にご提供しています。 AWS KMS(Key Management Service)： https://aws.amazon.com/kms/ AWS CloudHSM(Cloud Hardware Security Module) https://aws.amazon.com/jp/cloudhsm/ AWSコンプライアンス・ウェブサイト： https://aws.amazon.com/jp/compliance/ AWSセキュリティ・ウェブサイト： https://aws.amazon.com/jp/security/ 認定やサードパーティによる保証： https://aws.amazon.com/jp/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/
				2.　記憶装置の故障等により、機器・部品を交換する場合には、交換対象の記憶装置等の機器・部品に金融機関等やその顧客の情報等の機密性の高いデータが残存している可能性があるため、これらの記憶装置等に対しても、データ消去も含めた十分な管理を行う必要がある。 ただし、契約中の記憶装置等の障害・交換における消去証明書の発行・取得については、クラウド事業者に対して情報提出要請や監査等の方法で消去・破壊プロセスの実効性を検証することで代替することも可能である。 管理策としては、以下のような例がある。	AWSでは、Amazon S3、Amazon EBS、Amazon SimpleDB、Amazon 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へのIPSecトンネルも暗号化されます。 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。 お客様は、サードパーティの暗号化テクノロジを使用することもできます。 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(国家産業セキュリティプログラム運営マニュアル)またはNIST 800-88(媒体のサニタイズに関するガイドライン)に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。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。詳細については、「AWSセキュリティプロセスの概要」ホワイトペーパー（http://aws.amazon.com/security）を参照してください。

基準大項目	中項目	項番	小項目	基準項目の目的　内容説明　具体例等の解説	AWSの情報
		運111	クラウド契約終了時のデータ漏洩防止策を講ずること。	1.　クラウドサービスの契約を終了する場合、金融機関等が自らデータを消去することが困難な場合であっても、クラウド事業者とともに機密保護、プライバシー保護及び不正防止のための対策を講ずることが必要である。【運75】	AWSでは、Amazon S3、Amazon EBS、Amazon SimpleDB、Amazon 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へのIPSecトンネルも暗号化されます。 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。 お客様は、サードパーティの暗号化テクノロジを使用することもできます。 AWS利用者はデータの統制と所有権を保持します。AWSは、AWS利用者に対して、AWS利用者のデータを削除する機能を提供しています。お客様の要件に応じてデータの保持を管理するのはお客様の責任です。詳細については、AWSセキュリティプロセスの概要ホワイトペーパー（http://aws.amazon.com/security）を参照してください。 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(国家産業セキュリティプログラム運営マニュアル)またはNIST 800-88(媒体のサニタイズに関するガイドライン)に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。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。詳細については、「AWSセキュリティプロセスの概要」ホワイトペーパー（http://aws.amazon.com/security）を参照してください。
				2.　データ消去にあたっては、以下の方法が考えられる。	
				3.　クラウド事業者がデータ消去を実行する場合は、消去証明書等を受領することが望ましい。 なお、クラウドサービス契約終了時において、クラウド事業者が論理的消去も含めたデータ消去を実施することを契約書に記載し、かつ外部の第三者が監査等において、消去プロセスの適切性を検証することにより、消去証明書の発行・取得の代替とすることも可能である。	
				4.　顧客データ等の機密情報を扱わない業務をクラウドに委ねる場合は、契約終了時のデータ消去プロセスを簡略化または不要とすることも考えられ、消去証明書を不要とすることも可能である。	

基準大項目	中項目	項番	小項目	基準項目の目的　内容説明　具体例等の解説	AWSの情報
		運112	クラウド事業者に対する立入監査・モニタリング態勢を整備すること。	1.　利用しているクラウドサービスについて、有効性、効率性、信頼性、遵守性及び安全性の面から把握、評価するため、システム監査やモニタリングを実施することが必要である。 システム監査・モニタリングについては【運90、運91】を参照のこと。	AWSでは、統制目標と統制の設計と運用効率の検証は、社内外の監査人がプロセスを実地検証し、証拠を評価することによって行われており、検証結果については、認定、その他サードパーティによる証明を通じて、当社のIT統制環境に関する幅広い情報をお客様にご提供しています。本文書は、お客様が使用するAWSサービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様にご理解いただくことをお手伝いするためのものです。この情報はまた、お客様の拡張されたIT環境内の統制が効果的に機能しているかどうかを明らかにし、検証するのにも有用です。 AWSコンプライアンス・ウェブサイト： https://aws.amazon.com/jp/compliance/ AWSセキュリティ・ウェブサイト： https://aws.amazon.com/jp/security/ 認定やサードパーティによる保証： https://aws.amazon.com/jp/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/
				2.　金融機関等は、自らの業務処理を自社の責任で適正に行い、顧客データ等の重要情報を適切に管理する必要があるため、業務委託を行う場合には、当該委託業務が適切に運営されているかを検証することが求められる。 この点について、情報提出依頼のみで委託業務の適切性の検証が十分にできない場合は、クラウド事業者のオフィスやデータセンターへの立入監査・モニタリング等により実地で確認することが必要である。	AWSのデータセンターは複数のお客様をホストしており、幅広いお客様が第三者による物理的なアクセスの対象となるため、お客様によるデータセンター訪問は許可していません。 このようなお客様のニーズを満たすために、 SOC1 Type II レポートの一環として、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的なセキュリティの個別の確認も、ISO 27001 監査、PCI 評価、ITAR 監査、FedRAMP[sm] テストプログラムの一部となっています。 AWSコンプライアンス・ウェブサイト： https://aws.amazon.com/jp/compliance/
				3.　委託元金融機関の立入監査等が実効的でない場合などには、第三者監査により代替することも可能である。その際に考慮すべき事項としては、以下のようなことが考えられる。	AWSセキュリティ・ウェブサイト： https://aws.amazon.com/jp/security/ 認定やサードパーティによる保証： https://aws.amazon.com/jp/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/
				4.　金融機関等において、業務の特性を十分に検討したうえで、委託する業務の重要度が高くないと判断し得る場合には、費用対効果を踏まえた管理策を講じることで、立入監査等に代替することも可能である。 例えば、以下のような方法が考えられる。	

基準大項目	中項目	項番	小項目	基準項目の目的　内容説明　具体例等の解説	AWSの情報
		運113	サイバー攻撃対応態勢を整備すること。	1.　サイバー攻撃に伴うシステムの停止や、不正な資金移動に対する、未然防止策・事前対策、検知策、対応策を検討し、態勢を整備することが必要である。また、以下に示す例の他に、各金融機関等でも有効と考えられるセキュリティ対策について検討することが必要である。	AWS は、すべてのサービスエンドポイント IP アドレスに接するインターネットの脆弱性を定期的にスキャンします (お客様のインスタンスはこのスキャンの対象外です)。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します。 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ます。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 上層部に報告されます。 さらに、AWS統制環境は、通常の内部的および外部的監査およびリスク評価によって規定されています。 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ます。 AWSコンプライアンス・ウェブサイト： https://aws.amazon.com/jp/compliance/
				2.　未然防止策・事前対策には、以下のような例がある。	AWSセキュリティ・ウェブサイト： https://aws.amazon.com/jp/security/ 認定やサードパーティによる保証： https://aws.amazon.com/jp/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/ また、対象をお客様のインスタンスに限定し、かつAWS利用に関する契約に違反しない限り、お客様はご自身のクラウドインフラストラクチャのスキャンを実施する許可をリクエストできます。
				3.　検知策には、以下のような例がある。	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、主要なオペレーションメトリックをモニタリングしています。重要計測値が早期警戒しきい値を超える場合に運用管理担当者に自動的に通知されるよう、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。 AWSのログおよびモニタリングプロセスは、SOC、PCI DSS、ISO27001、および FedRAMP コンプライアンスへの AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。また、AWSは、ホワイトペーパー、認定、その他サードパーティによる証明を通じて、当社のIT統制環境に関する幅広い情報をお客様にご提供しています。 AWSコンプライアンス・ウェブサイト： https://aws.amazon.com/jp/compliance/ AWSセキュリティ・ウェブサイト： https://aws.amazon.com/jp/security/ 認定やサードパーティによる保証： https://aws.amazon.com/jp/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/ また、AWSはサービスの稼働状況に関する最新情報を、サービスヘルスダッシュボードで提供しています。 http://status.aws.amazon.com AWS利用者はゲストOS、ソフトウェア及びアプリケーションをコントロールし、監視手順を定義する責任があります。AWS Cloudwatch は AWS のクラウドリソースや利用者がAWS上で動作させているアプリケーションに対する利用者 による監視の機能を提供します。 Amazon CloudWatch： http://aws.amazon.com/cloudwatch AWS利用者は所有するIDの不正使用を制限する権利と責任を保持します。AWSのアイデンティティ及びアクセス管理 (IAM) サービスは、アイデンティティの管理機能をAWS管理コンソールに提供します。 http://aws.amazon.com/mfa

基準大項目	中項目	項番	小項目	基準項目の目的　内容説明　具体例等の解説	AWSの情報
				4.　対応策には、以下のような例がある。	障害の理由にかかかわらず、AWSでは、対応手順や連絡手順等についてホワイトペーパー、インターネット上のウェブサイト、レポート、認定、その他サードパーティによる証明を通じて、当社のIT統制環境に関する幅広い情報をお客様にご提供しています。 AWSウェブサイト： https://aws.amazon.com/ AWSコンプライアンス・ウェブサイト： https://aws.amazon.com/jp/compliance/ AWSセキュリティ・ウェブサイト： https://aws.amazon.com/jp/security/ 認定やサードパーティによる保証： https://aws.amazon.com/jp/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/
				5.　教育・訓練には、以下のような例がある。	すべての従業員は企業理念に沿った行動と倫理を行なうよう、定期的な情報セキュリティの訓練を行ない、それの完了の承認を得る必要があります。定期的に行なわれるコンプライアンスの監査は、これらを従業員が理解し、確立されたポリシーに従っていることを検証するために実施されます。詳細については、「AWSセキュリティ·プロセスの概要」のホワイトペーパーを参照してください。http://aws.amazon.com/security AWS は、英国政府の支援により業界がサポートする英国発の認定 Cyber Essentials Plusを取得しており、英国政府が 提供する「10 Steps to Cyber Security（サイバーセキュリティへの10 ステップ）」 のコンテキスト内で、 一般的なインターネットベースの脅威がもたらすリスクを緩和するためにAWSが実装しているベースライン コントロールを示しています。 詳細については、ホワイトペーパーをご参照ください。
				6.　サイバー攻撃に対応するためには、事前の情報収集並びに攻撃発生時の相談先として、セキュリティ対応機関を利用することが望ましい。	AWSコンプライアンス・ウェブサイト： https://aws.amazon.com/jp/compliance/ AWSセキュリティ・ウェブサイト： https://aws.amazon.com/jp/security/