金融機関向け「Amazon Web Services」対応セキュリティリファレンス

金融情報システムセンター（FISC）「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版および第8版追補改訂」対応
version 1.30

2016/11/10

作成：SCSK株式会社
株式会社電通国際情報サービス
株式会社野村総合研究所
TIS株式会社
三井情報株式会社
トレンドマイクロ株式会社
株式会社シーエーシー
株式会社ワークスアプリケーションズ
JBCC株式会社

最終更新日 2016/11/10

Version	改版内容	更新日
1.00	新規作成	2012/9/10
1.10	クラウド特有の対応方法を追加。	2013/3/18
1.20	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版および第8版追補対応	2013/9/11
1.30	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版および第8版追補改訂対応	2016/11/10

金融機関がAWSを利用してシステムを構築する場合、セキュリティ事項の事前確認をサポートするために、FISCの各安全対策基準（第8版追補改訂）の項目のうち、クラウドおよびサイバー関連の項目について、【対応の主体】、【対応可否判断のための情報参照元】、【AWSの該当情報】、【確認した内容と解説】の分類で整理した。

【対応の主体】
「クラウド事業者」ならびに「利用者」のそれぞれが対応すべき項目を”〇”、そうでない項目を”ー”として整理した。

【対応可否判断のための情報参照元】
FISCのガイドラインに沿って、該当するAWSのホワイトペーパー等の公開情報から記載。
なお、情報参照元は各社が確認を行った時点のもので、ご利用時に参照できないあるいは内容が変更となっている場合がある。

【AWSの該当情報】
各項目についてのAWSの説明。AWSの対応方針やAWSの提供しているソリューション。

【確認した内容と解説】
パートナー各社がAWSからの公開情報や対応方針、ソリューションの説明について、NDA情報やインタビューを含めて確認、整理した結果を記載した。
なお、「NDA情報」とはAWSとの秘密保持契約の締結にもとづき提供される各種報告書等を指す。（例：SOC1監査報告書、SOC2監査報告書等）

※【FISC安全対策基準への適合性】
従来版では適合性の判定結果を表示してきたが、今回FISCによりリスクベースアプローチの考え方が全面的に導入され、
利用する業務の特性・重要度に応じた利用金融機関の判断が求められることになったことを受け、誤読の可能性を考慮し廃止した。

	FISC 安全対策基準第8版および第8版追補改訂からの引用							対応の主体		対応可否判断のための情報参照元	AWSの該当情報	確認した内容と解説
	項番	基準大項目	基準中項目	基準小項目	適用にあたっての考え方	基準項目の目的 内容説明 具体例等の解説	基準項目の目的 内容説明 具体例等の解説	クラウド事業者	利用者	基準項目に対するクラウド事業者の一般公開情報の所在		
A38720001	運108	V. 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。	クラウドサービスの利用を行う場合は、事前に目的や範囲等を明確にするとともに、クラウド事業者の選定に際しては手続きを明確にし、事業者を客観的に評価すること。 また、事業者の決定にあたっては、責任者の承認を得ること。	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。		—	○	N/A(利用者側対応事項)	–	金融機関側でクラウドサービス利用、クラウド事業者選定手続きの整備が必要である。
A38720002	運108	V. 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。	クラウドサービスの利用を行う場合は、事前に目的や範囲等を明確にするとともに、クラウド事業者の選定に際しては手続きを明確にし、事業者を客観的に評価すること。 また、事業者の決定にあたっては、責任者の承認を得ること。	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。	(1) 利用目的 (2) 利用業務範囲 (3) 利用形式 (4) 利用期間 (5) 利用費用 (6) リスクの管理方法 (7) クラウド事業者の選定条件 (8) クラウドサービスに関する自社窓口と役割 等	—	○	N/A(利用者側対応事項)、10	–	金融機関側で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確認する必要がある。(金融機関におけるクラウド利用に関する有識者検討会報告書【図表G】を参照)
A38720003	運108	V. 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。	クラウドサービスの利用を行う場合は、事前に目的や範囲等を明確にするとともに、クラウド事業者の選定に際しては手続きを明確にし、事業者を客観的に評価すること。 また、事業者の決定にあたっては、責任者の承認を得ること。	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。	(1) クラウド利用を想定する業務に係る実績、技術レベル 1) 信頼度及び受託実績(類似システムの開発実績、他プロジェクトやサービスでの評判等) 2) 技術レベル(業務内容の理解度、業界に関する知識(金融機関等が委託する業務に関する専門性)、情報収集能力、プロジェクト管理能力(クラウド事業者が安定して業務に係る開発・運用をしているか等)、導入サポート力等)	○	○	3、4	AWSは、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ホームページ: https://aws.amazon.com/ AWSホワイトペーパー: https://aws.amazon.com/jp/whitepapers/ AWSアナリストレポート: https://aws.amazon.com/jp/resources/analyst-reports/ 責任共有モデル: https://aws.amazon.com/jp/compliance/shared-responsibility-model/ 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/	第三者のアナリストレポートや顧客事例等により、金融機関によるクラウド事業者客観的評価に必要な情報が、AWSより提供されている事を確認した。また必要な手続きをとることで、第3者監査レポート等の非公開情報も直接受領できることを確認した。
							(2) 事業継続性(経営方針、経営体力・収益力、人的基盤、被災時のBCM・データのバックアップ)			5、11、9		公開文書及びNDA情報により、AWSの事業継続性(経営方針、経営体力・収益力、人的基盤、被災時のBCM・データのバックアップ)に関する情報が提示されていることを確認した。
							(3) サービスの可用性・データの安全性(機密性保護)・完全性の確保のための態勢、セキュリティ対策の実施状況(機密保護状況を含む)			5、9、15、16、13		公開文書及びNDA情報により、AWSのサービスの可用性・データの安全性(機密性保護)・完全性の確保のための態勢、セキュリティ対策の実施状況(機密保護状況を含む)に関する情報が提示されていることを確認した。
							(4) 内部統制やリスク管理等に関する状況(再委託先管理も含む)、外部監査の受検や各種公的認証の取得状況、組織体制(コンプライアンス体制を含む)			5		公開文書及びNDA情報により、AWSの内部統制やリスク管理等に関する状況(再委託先管理も含む)、外部監査の受検や各種公的認証の取得状況、組織体制(コンプライアンス体制を含む)に関する情報が提示されていることを確認した。
							(5) 情報開示姿勢			1、2、5		公開文書により、AWSのセキュリティ対策やコンプライアンス等に関する情報が開示されていることを確認した。また、第三者監査人が作成したレポート及び認定書をリクエストして入手できることも確認した。
							(6) 立入監査の受入に関する方針、訪問調査の受入スタンス、コミュニケーションルート			5		公開文書により、AWSは金融機関による立入監査は受入れない方針で、代替として第三者監査人が作成したレポートをNDA締結により開示していることを確認した。リクエストによりSOC 1 Type II レポートが入手できることも確認した。
							(7) データの所在(データが保管される場所、または保管の可能性がある場所)			5		公開文書により、AWSがクラウドサービスに適用される法令が特定できる範囲の国、州等のレベルでデータの所在を明らかにしているが、詳細な所在地についてはセキュリティ確保の観点から明らかにいない方針であることを確認した。
							(8) 既存システムとの連携・新システムへのデータ移行の容易性			17		公開文書により、AWSのAPIやサービスを使用することで、クラウドサービスの既存システムとの連携及び新システムへのデータ移行の容易性を実例を含めて確認した。
							(9) 保守体制・サポート体制(サポートデスク、問題発生時の対応力(障害発生時におけるトレーサビリティの確保等)、日本語での対応)			21 サービス利用者へのサポート、22		公開文書により、AWSのサポート(レベル別に緊急度により最初の連絡までの応答時間が明示される等)の提供と、保守体制・サポート体制があることを確認した。
							(10) インシデントが発生した場合の想定損害額(直接損害・間接損害)とクラウド事業者側が提示する損害賠償・補償上限額とのバランス			21 責任限定		公開文書により、AWSが提示する損害賠償・補償上限額が、かかる請求に先立つ12ヶ月分の実際の支払額であることを確認した。
							(11) サービス利用廃止時の対応(ベンダーロックインリスク対応、データ消去等) ただし、契約の中断・終了に伴うシステム移行作業(移行データの抽出方法と実際の移行作業内容)については、サービス利用前に把握することが望ましい。			21 停止,.契約期間および契約解除、5		公開文書により、金融機関は、データの統制と所有権を保持しており、また必要に応じて、金融機関がAWSストレージからデータを出し入れする可搬性をAWSが許可していることを確認した。 また、サービス契約解除後のAWSサービス環境からのデータ取り出し時の支援方針が明示されていることも確認した。
							(12) 個人データの取扱いの全部または一部を事業者に行わせることを内容とする契約を締結する場合は、「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」のⅢに定める「個人データ保護に関する委託先選定の基準」に準拠対応可能か			21 データプライバシー		公開文書により、金融機関は、データの統制と所有権を保持しており、データの外部委託に該当しないという考えであることを確認した。
							(13) 委託費と支払い条件			21 料金及び支払い		公開文書により、委託費用と支払い条件について確認した。
							なお、(5)情報開示姿勢の中でも、リスク管理に直結する事項(注)については、十分に把握しておくことが必要である。このため、こうした情報の開示が必ずしも十分でないクラウド事業者と契約してよいか、慎重な判断が必要である。 (注) リスク管理に直結する事項には以下のようなものがある。 1) データの入力・保管・処理・バックアップ・出力といった一連のフロー 2) 暗号方式、暗号化領域、非暗号化領域 3) ログ(システムログ、業務ログ、操作ログ等)の取得範囲・取得頻度・保存期間・開示範囲 4) バックアップを含むデータコピーの取得内容・保管場所・保管期間 等			–		–
A38720004	運108	V. 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。	クラウドサービスの利用を行う場合は、事前に目的や範囲等を明確にするとともに、クラウド事業者の選定に際しては手続きを明確にし、事業者を客観的に評価すること。 また、事業者の決定にあたっては、責任者の承認を得ること。	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		○	○	21 準拠法,裁判地、5	準拠法に関しては、AWSカスタマーアグリーメントを参照ください。 https://aws.amazon.com/jp/agreement/ 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。S3データオブジェクトのデータレプリケーションは、データが保存されているリージョンのクラスタ内で実行され、他のリージョンの他のデータセンタークラスタにはレプリケートされません。データとサーバ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、法令遵守または政府機関の要請によりやむをえない場合を除き、お客様のコンテンツを指定されたリージョンからお客様への通告なしに移動することはありません。2016年11月時点では、リージョンは14あります。米国東部(バージニア北部)、米国西部(オレゴン)、米国西部(北カリフォルニア)、米国東部(オハイオ)、AWS GovCloud(米国)(オレゴン)、欧州(アイルランド、フランクフルト)、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)、アジアパシフィック(ソウル)、アジアパシフィック(ムンバイ)、中国(北京)、南米(サンパウロ)です。 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、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、FedRAMPsm テストプログラムの一部となっています。	公開文書により、準拠法は、アメリカ合衆国ワシントン州法であることを確認した。またインタビューにより金融機関の個別の要望について相談が可能であることを確認した。 公開文書により、データとサーバーを配置する物理的なリージョンは、金融機関が指定可能で、AWSは、法令遵守または政府機関の要請によりやむをえない場合を除き、金融機関のコンテンツを指定されたリージョンから金融機関への通告なしに移動することはしない方針であることを確認した。
A38720005	運108	V. 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。	クラウドサービスの利用を行う場合は、事前に目的や範囲等を明確にするとともに、クラウド事業者の選定に際しては手続きを明確にし、事業者を客観的に評価すること。 また、事業者の決定にあたっては、責任者の承認を得ること。	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。	(1) 現地の各種法制や制度の把握と分析	○	○	21 準拠法,裁判地	—	
							(2) 現地での活動資格を有する弁護士の確保			21 準拠法,裁判地	–	
							(3) 地理不案内な遠隔地での打合せや出廷などに伴う経済的、人的負担			21 準拠法,裁判地	–	
							(4) 上記すべてについての外国語での対応			21 完全合意	–	
A38720006	運108	V. 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。	クラウドサービスの利用を行う場合は、事前に目的や範囲等を明確にするとともに、クラウド事業者の選定に際しては手続きを明確にし、事業者を客観的に評価すること。 また、事業者の決定にあたっては、責任者の承認を得ること。	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。		—	○	N/A(利用者側対応事項)	–	金融機関側で、クラウド事業者の選定の決裁権限の明文化が必要となることを確認した。
A38720007	運108	V. 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。	クラウドサービスの利用を行う場合は、事前に目的や範囲等を明確にするとともに、クラウド事業者の選定に際しては手続きを明確にし、事業者を客観的に評価すること。 また、事業者の決定にあたっては、責任者の承認を得ること。	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。		○	○	5	IT インフラストラクチャを AWS に移行すると、お客様と AWS の責任分担モデルを構成します。この共有モデルは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、様々なコンポーネントを AWS が運用、管理、およびコントロールするというものです。このため、お客様の運用上の負担を軽減する助けとなることができます。お客様の責任としては、ゲストオペレーティングシステム(更新やセキュリティパッチなど)、その他の関連アプリケーションソフトウェア、ならびにAWSより提供されるセキュリティグループファイアウォールの設定の責任と管理が想定されます。	AWSの提供するサービス等の導入に際し、金融機関は必要に応じ、【運72、運73】のパッケージソフトの選定にかかる評価体制及び運用・管理体制の整備を参照することが必要となることを確認した。
A38730001	運109	V. 運用基準	クラウドサービスの利用	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。	安全性確保のため、機密保護、安定的なシステム運用等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。	(1) 基本的な事項 1) 用語の定義、役割分担、責任範囲、債務不履行時の損害賠償範囲、準拠法、裁判管轄等 2) 検収、納品の条件と手順、及び権利の移転の時期 3) 品質の保証と確認手順 4) 作業時間、立入場所等 5) 指示目的外使用 6) 契約変更の場合の手順 7) 仕様変更の取扱い	○	○	21、23、25	—	(運用109共通) 簡易な管理が求められる場合には、公開文書によりAWSの標準のカスタマーアグリーメント、各種SLAですぐにでもAWSが利用可であることを確認した。 厳格な管理が求められる場合には、金融機関の個別の要望について相談が可能であることを確認した。
							(2) 個別契約条件、サービス仕様、データ保護の管理策 1) 利用する業務の期限、費用 2) クラウド事業者(複数のクラウド事業者がサービスの委託を受けた場合も含む)との間の管理境界や責任分界点に関する取決め(注) (注) クラウドサービスには、複数のクラウド事業者がサービスの委託を受けることがある。こうした状況下では、特定のクラウド事業者が所管するリソースにおける性能面のボトルネックや障害がクラウドサービス全体の品質に甚大な影響を与え得ることに留意する必要がある。インシデントが発生した場合に、それぞれのクラウド事業者が自らの責任の所在を認めず、責任の擦り付け合いが生じ、その結果、障害の状況把握や復旧対応が遅延するといった事態を回避しなければならない。 3) サービス仕様(リソースの割当て等(仕様上の制限や変更に必要な時間等)) 4) 機密保護 5) 金融機関等が守るべき法令や金融機関等のセキュリティポリシー等、クラウド事業者の要員が遵守するべきルール 6) セキュリティ管理方法及び体制 7) クラウドサービスを利用するためのデータのバックアップ	○	○	21 全般、21 提供される本サービス内容の変更、23	—	
							(3) サービスレベル未達の場合の対応	○	—	5 、21 全般	—	

FISC 安全対策基準第8版および第8版追補改訂からの引用								対応の主体		対応可否判断のための情報参照元	AWSの該当情報	確認した内容と解説
	項番	基準大項目	基準中項目	基準小項目	適用にあたっての考え方	基準項目の目的 内容説明 具体例等の解説	基準項目の目的 内容説明 具体例等の解説	クラウド事業	利用者	基準項目に対するクラウド事業者の一般公開情報の所在		
							(4) 情報開示範囲、監督当局等による検査等への協力義務、金融機関による監査受入、事業者と利用者間の報告・連絡等の運営ルール、インシデントレスポンスの取扱い 1) 作業の報告方法と報告形式 2) 作業の指示に関する取決め 3) 利用する業務における問題発生時の解決体制 4) 保守及び障害時等の回復作業・復旧手順、マニュアル整備及び教育・訓練 5) 目標復旧時間(RTO:Recovery Time Objective) 6) 事故発生時における報告 7) 情報漏洩等のインシデントが発生、もしくは発生が疑われる場合における、トレーサビリティ確保のための調査協力義務 8) 利用する業務におけるクラウド事業者での対策を含むコンティンジェンシープラン(緊急時対応計画)	○	○	—	—	
							(5) 反社会的勢力・テロ組織と関わりがないことの表明・確約	○	—	—	—	
							(6) 利用終了時の原状回復・新システム移行時の協力義務、データの返却・消去等 1) 契約の解除条件(クラウド事業者の業務遂行に問題がある場合に、他のクラウド事業者等と契約する権利等) 2) サービス契約終了時におけるクラウド事業者によるデータの消去の実施、将来的なハードウェア更改・撤去時におけるデータの物理的消去の実施、データ消去の実施時期や消去証明書の発行時期[運111]3. 3) サービス契約終了時における原状回復・データ移行作業等の協力義務	○	—	5	—	公開文書により、 契約解除条項やデータ移行作業等の協力、データの保持条項を確認した。
							(7) 損害が発生した場合の協議や賠償に関する取決め	○	—	21 責任限定	—	公開文書により、損害発生時の協議や賠償限度額の規程を確認した。
							(8) クラウド事業者のサービスを利用した結果の知的財産権や使用権等の権利の帰属 ただし、以下の事項は契約に明記することが望ましい。	○	—	21 所有権等	—	公開文書により、知的財産権や使用権等の権利の帰属の規程を確認した。
							(9) クラウド事業者からの情報開示 1) 平常時における標準的な情報開示内容の明記 クラウド事業者が複数の委託元金融機関から多種多様な開示請求を受けた場合、対応負担が増す可能性がある。このため、事前にある程度標準的な情報開示の範囲を契約またはSLA等で定めることにより クラウド事業者の負担軽減を図り、金融機関からの情報開示の請求に対応しやすくする旨の記述をすることが望ましい。クラウド事業者によっては一般に公開している内容以上の情報提供について、その機密性の保全目的もあり非現的なケースがあるため、金融機関による情報開示請求があった場合には、その必要性の説明が合理的である限り、金融機関とクラウド事業者が協議のうえ、必要な情報をクラウド事業者が提供することを契約上明記すること。開示請求の対象情報の機密性が高い場合には、両者の間で機密保持契約を締結したうえで提供すること。 2) リスク顕在化時の情報開示 リスク事象が発生した際、または各種の資料により情報漏洩リスクが高まった、もしくはクラウド事業者側の内部統制状況が悪化したなどと判断される場合、平常時における標準的な情報開示の前提に関わらず、金融機関からの開示請求を受けたときには、請求内容に応じた情報開示を行っていくべきことを契約やSLAに明記すること。 なお、金融機関等において、業務の特性を十分検討したうえで、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、クラウド事業者に対し、リスク管理に直結する事項等の情報を詳細かつ厳格に求めないことも可能である。この場合には、クラウド事業者が提示する標準的な情報開示の内容で十分であり、さらに付加的な情報を求めないことも考えられる。	○	—	5 、1	—	簡易な管理が求められる場合には、AWSの公開文書による標準的な情報開示ですぐにでもAWSが利用可であることを確認した。 厳格な管理が求められる場合のAWSの情報開示について以下のとおり確認した。 1)平常時の情報開示について、公開文書及びNDA締結による第三者監査レポートの提供を確認した。 2)リスク顕在時の情報開示規定明文化については、各金融機関の個別の要望について相談が可能であることを確認した。
A38730001	運109	V. 運用基準	クラウドサービスの利用	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。	安全性確保のため、機密保護、安定的なシステム運用等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。	(10) 複数のクラウド事業者への委託 クラウドサービスには、複数のクラウド事業者がサービスの委託を受けることがある。こうした状況下では、特定のクラウド事業者が所管するリソースにおける性能面のボトルネックや障害がクラウドサービス全体の品質に甚大な影響を与えうることに留意すること。インシデントが発生した場合に、それぞれのクラウド事業者が自ら責任の所在を認めず、責任の擦りつけ合いが生じ、その結果、障害の状況把握や復旧対応が遅延するといった事態を回避しなければならない。 このため、障害発生時等の迅速な対応のため、委託元金融機関の管理能力を踏まえ、委託元金融機関・クラウド事業者間での責任関係を明確にし、一元的な窓口機能やクラウド事業者間の相互調整機能を担う事業者をあらかじめ決めておくこと。なお、この役割を委託元金融機関が担える場合においては、クラウド事業者側の相互調整機能を必ずではないなお、金融機関等において、業務の特性を十分検討したうえで、委託する業務の重要度が高くないと判断し得る場合、かつリスク分析の結果として、障害発生時の影響範囲が限定的である、もしくは復旧自体が遅れてもその影響が軽微であると判断し得る場合は、相互調整を担う事業者を置かないことも可能である。	○	—	5	—	公開文書により、AWSはサードパーティのプロバイダーサービスは一切使用していないことを確認した。
							(11) 再委託管理 1) 再委託先に対する金融機関等の事前審査 金融機関等は、安定したサービスの継保や情報保護等のために、直接の委託先であるクラウド事業者のみならず、再委託先についても同様に実態把握し適切なリスク管理を行うこと。 ・委託の状況を把握し、不適切な再委託先が介在することを排除するため、委託業務を再委託する場合、再委託先に対する適切な事前審査を行うこと(注1)。 (注1) 金融機関が自ら事前審査を行う場合、事前審査作業を効率化するため、クラウド事業者側と金融機関側の合意により、あらかじめ、再委託先の候補先企業群に対し事前審査を行うという工夫を講じることも考えられる。 ・再委託先に対する事前審査については、例えば、クラウド事業者による再委託先の審査・管理プロセスが金融機関のそれよりも実効的であるとみなされる場合には、クラウド事業者側での事前審査が最適となり得る点には留意が必要である(注2)。なお、助言系システムや機密性の高い顧客データを保管するシステム等、特に重要な業務を再委託する場合には、金融機関等自らが事前審査をすること。 (注2) クラウド事業者側での再委託先の審査については、金融機関のリスク管理ポリシー等と照らし、金融機関自らが行う審査と比較して、その範囲・深度について同等かそれ以上である必要がある。これが満たされる場合は、個別の再委託先(既存分、新規追加・変更分)に係る事前報告や承諾を必ずしも要しない。 2) 損害賠償も含めた責任の明確化 再委託先が問題を発生させた際、速やかな復旧回復の責任を負うことと同時に、委託先が損害賠償上限条項に定められた範囲内で賠償責任を負うことを明確にすること。 3) 委託先・再委託先間の義務の明確化 委託先が金融機関に対して負う義務報告・内部統制確保義務などの各種義務を再委託先も負う扱いとするため、委託先・再委託先間の契約に必要な義務に関する条項を設けることを金融機関と委託先との契約に明記すること。 4) 再委託の中止の扱い 各種の報告資料等を踏まえ、再委託先の業務遂行能力に対し、問題視し得る状況が生じた場合、金融機関はクラウド事業者に対し、再委託の中止を求めることができることを明確にし、契約上明記することが望ましい。クラウド事業者が中止の求めに応じない場合は、サービス利用の停止も検討すること。 なお、金融機関等において、業務の特性を十分検討したうえで、委託する業務の重要度が高くないと判断し得る場合は、再委託先における委託元金融機関による事前の審査や日常のモニタリング等のリスク管理を簡易化することも可能である(注)。例えば、再委託する対象業務が重要な業務ではなく、サイバー攻撃対策や内部不正による情報漏洩対策などのリスク管理及びログの取得・分析を含めたインシデント発生時の緊急対応を直接の委託先であるクラウド事業者側で行うといった場合などが該当するという判断も可能である。 (注) リスク管理の簡易化については、例えば、チェック項目や頻度、深度の軽減化が考えられる(ただし、反社会的勢力等については、社会的に厳格な対応が求められていることに留意すること)。	○	○	5 サードパーティの利用と審査	—	簡易な管理が求められる場合には、厳格な事前審査は必須でなく、必要に応じた再委託先のチェック、モニタリングが金融機関に求められる、またクラウド事業者側の審査の方が実効的である場合には、クラウド事業者側の審査で代替することも可能であることを確認した。 公開文書により、AWS サードパーティの要件は、PCI DSS、ISO 27001、および FedRAMPsm への準拠のため、監査中に外部の独立監査人によって確認されることを確認した。 厳格な管理が求められる場合には、各金融機関の個別の要望について相談が可能であることを確認した。
A38730001	運109	V. 運用基準	クラウドサービスの利用	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。	安全性確保のため、機密保護、安定的なシステム運用等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。	(12) 委託元金融機関による立入監査・モニタリング【運112】 1) 立入監査等の権利の明記 業務委託契約に、委託元金融機関等の立入監査等を実施する権利を明記すること。 2) 立入監査等の代替手段 委託元金融機関が直接、立入監査等を実施するのではなく、平常時には立入監査等のスキルのある外部の第三者による検証により代替することも可能とすること。 3) 立入監査等の権利行使 クラウド技術に関する重要な脆弱性が判明した場合、クラウド事業者における他の顧客に関わる領域でインシデントが発生した場合、他事業者でインシデントが発生した場合等に、委託元金融機関への影響を確認するため、臨時の第三者監査を行うことが可能となっていること。 なお、立入監査等に代替する第三者監査が行われない、または依拠できないと判断される場合に限定して立入監査等を行う運用形態を取る場合は、立入監査等の権利行使の条件を必要に応じ書面化し、委託元金融機関とクラウド事業者の両者が認識を共有することも可能である。 4) 立入監査等の受入対応費用 立入監査を受けるクラウド事業者側の受入対応の費用については、委託元金融機関、クラウド事業者側のいずれが負担するか、あらかじめ両者で協議しておくこと。 5) 再委託先への立入監査等 再委託する業務が重要な場合、再委託先等に対して、委託元金融機関とクラウド事業者間の契約に、金融機関による再委託先への立入監査を実施する権利を明記すること。 6) 立入監査等の指摘事項の扱い 立入監査等により判明した指摘事項については、対応の是非を含め、委託元金融機関とクラウド事業者の両者で協議のうえ、合理的な対応期間を定め、期間内に対応する旨をあらかじめ契約上明確にすること。	○	○	5,25	AWSカスタマーアグリーメントは、お客様のサービス利用に提供されます。 https://aws.amazon.com/jp/legal/ AWSはお客様にAWSサービスを提供するにあたり、サードパーティのクラウドプロバイダは一切使用していません。 AWSは、いくつかの業界の認定と独立したサードパーティによる証明を取得し、いくつかの認定、レポートなどの関連する文書を、NDA に従って AWS のお客様に直接提供しています。 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、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、FedRAMPsm テストプログラムの一部となっています。 ほとんどのレイヤーと、物理統制よりも上の統制の監査は、お客様の担当です。AWS 定義の論理統制と物理統制の定義は、SOC 1 Type II レポート(SSAE 16)に文書化されています。また、このレポートは、この監査チームとコンプライアンスチームのレビューに使用できます。また、AWS ISO 27001 およびその他の認定も、監査人のレビュー用に使用できます。 なお、個別のご要求については、ご相談が可能です。	簡易な管理が求められる場合には、公開文書によりAWSの標準のカスタマーアグリーメント、各種SLAですぐにでもAWSが利用可であることを確認した。 厳格な管理が求められる場合には、NDA締結により立入監査、立入調査の代替となる第3者監査レポートが、提供されることを確認した。
							(13) 金融監督当局の検査等 金融監督当局は、当該金融機関の業務の健全性について、委託業務も含めて検証する公益上の要請がある。当局の要請があった場合、クラウド事業者としては立入検査等を受け入れることが法律上求められる。 1) 当局検査等への協力義務 当局の立入り検査等の円滑な実施を担保するため、委託元金融機関とクラウド事業者との間の契約に、クラウド事業者の当局検査等への協力義務を明記すること。 2) 再委託先への立入り検査等 業務委託の再委託先(再々委託先を含む)に対しても、金融機関と元請け事業者との間の契約に、当局検査等への協力義務を明記すること。 3) 検査等後の指摘事項の扱い 当局検査等の指摘事項については、速やかに改善を図る旨の条項を契約に明記すること。	○	○	5、25	AWSカスタマーアグリーメントは、お客様のサービス利用に提供されます。 https://aws.amazon.com/jp/legal/ AWSはお客様にAWSサービスを提供するにあたり、サードパーティのクラウドプロバイダは一切使用していません。 AWSは、いくつかの業界の認定と独立したサードパーティによる証明を取得し、いくつかの認定、レポートなどの関連する文書を、NDA に従って AWS のお客様に直接提供しています。 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、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、FedRAMPsm テストプログラムの一部となっています。 ほとんどのレイヤーと、物理統制よりも上の統制の監査は、お客様の担当です。AWS 定義の論理統制と物理統制の定義は、SOC 1 Type II レポート(SSAE 16)に文書化されています。また、このレポートは、この監査チームとコンプライアンスチームのレビューに使用できます。また、AWS ISO 27001 およびその他の認定も、監査人のレビュー用に使用できます。 なお、個別のご要求については、ご相談が可能です。	

FISC 安全対策基準第8版および第8版追補改訂からの引用								対応の主体		対応可否判断のための情報参照元	AWSの該当情報	確認した内容と解説
	項番	基準大項目	基準中項目	基準小項目	適用にあたっての考え方	基準項目の目的 内容説明 具体例等の解説	基準項目の目的 内容説明 具体例等の解説	クラウド事業	利用者	基準項目に対するクラウド事業者の一般公開情報の所在		
A38730001	運109	V. 運用基準	クラウドサービスの利用	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。	安全性確保のため、機密保護、安定的なシステム運用等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。	(14) インシデント発生時の立入調査 1) 情報漏洩等のインシデントが発生した場合、もしくは発生が疑われる場合に、クラウド事業者が情報提供に応じない、提供しても迅速性に問題があると金融機関が判断した場合、もしくは提出情報の網羅性に疑義が有る場合は、委託元金融機関自ら、もしくは委託元金融機関が指定するセキュリティ業者・デジタルフォレンジック業者の立入調査が実施できることについて、契約上明記すること。 2) 調査時に収集の対象となる証跡の範囲(クラウド事業者の他の顧客にかかわる証跡のため委託元金融機関に一般的には開示できないものも含む)及び抽出ツールの開発・検証のために必要となる費用負担(注)について、契約締結時に合意を得ること。 (注) クラウド事業者側が自らのポリシーにより、委託元金融機関の立入調査人や金融機関の指定するセキュリティ業者・デジタルフォレンジック事業者による機器操作のための調査受入を避けたい場合は、トレーサビリティを確保するため、委託元金融機関の施設、クラウド事業者側の施設、または外部施設の何れかにおいて解析に必要な情報を抽出することのできるツールが必要となる。また、これらの抽出ツールが適切に作動することに関する外部の第三者による検証を受けることが必要である。こうしたデータ抽出の機能は、アプリケーションの一部機能としてユーザーに提供されるケースもあるが、提供されていない、ないし網羅性に問題がある場合は、別途、抽出ツールの開発・検証が必要になる。この場合、委託元金融機関としては、収集の対象となる証跡の範囲(当該クラウド事業者の他の顧客にかかわる証跡のため委託元金融機関に一般的には開示できないものも含む)や抽出ツールの開発・検証のために必要となる費用負担について、契約締結時にクラウド事業者とあらかじめ合意を得る必要がある。 3) クラウド事業者の経営不安が発生した場合、委託元金融機関自らもしくは委託元金融機関が指定する専門業者が、必要に応じ、クラウド事業者施設に立ち入り、顧客データや関連資作物・成果物の保全を行うことを認めるよう契約に明記すること。 なお、金融機関等において、業務の特性を十分検討したうえで、委託する業務の重要度が高くないと判断し得る場合は、費用対効果を踏まえた管理策を講じることで立入に代替することも可能である。【運112】4.	○	○	5.25	AWSカスタマーアグリーメントは、お客様のサービス利用に提供されます。 https://aws.amazon.com/jp/legal/ AWSはお客様にAWSサービスを提供するにあたり、サードパーティのクラウドプロバイダは一切使用していません。 AWSは、いくつかの業界の認定と独立したサードパーティによる証明を取得し、いくつかの認定、レポートなどの関連する文書を、NDA に従って AWS のお客様に直接提供しています。 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、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、FedRAMPsm テストプログラムの一部となっています。 ほとんどのレイヤーと、物理統制よりも上の統制の監査は、お客様の担当です。AWS 定義の論理統制と物理統制の定義は、SOC 1 Type II レポート(SSAE 16)に文書化されています。また、このレポートは、この監査チームとコンプライアンスチームのレビューに使用できます。また、AWS ISO 27001 およびその他の認定も、監査人のレビュー用に使用できます。 なお、個別のご要求については、ご相談が可能です。	

	項番	基準大項目	基準中項目	基準小項目	適用にあたっての考え方	基準項目の目的 内容説明 具体例等の解説	基準項目の目的 内容説明 具体例等の解説	対応の主体 クラウド事業者	対応の主体 利用者	対応可否判断のための情報参照元 基準項目に対するクラウド事業者の一般公開情報の所在	AWSの該当情報	確認した内容と解説
							(15) 記憶装置等の障害・交換 ・記録媒体等を障害や交換等の事情により施設外へ持ち出す場合には、記録済データをあらかじめ復元が不可能または著しく困難な状態にしておくこと。【運110】	○	—	9	—	AWS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を含む処理手順を定めていることを確認した。
							(16) 海外でのデータ保管時の留意点 ・金融機関における障害対応要員の現地の語学力が十分でない場合、日本語でのサポート、クラウド事業者の日本法人等の障害対応窓口設置を明確にすること。	○	○	5	—	公開文書により、データとサーバーを配置する物理的なリージョンは、金融機関が国内のデータ保管を指定可能であることを確認した。また、AWSは、法令遵守または政府機関の要請によりやむをえない場合を除き、金融機関のコンテンツを指定されたリージョンから金融機関への通告なしに移動することはしない方針であることを確認した。
							(17) トレーサビリティの確保 クラウドは、仮想化され、かつ動的に変化する環境であるため、万一障害や情報漏洩等のインシデントが発生した際には、流出・毀損したデータの特定や原因究明のための作業が複雑化する場合があることが想定されるため、トレーサビリティ確保のための方策を準備すること。	○	○	16 セキュリティモニタリング,アラート,監査証跡,およびインシデント対応の管理	—	公開文書により、AWSでは万一障害や情報漏洩等のインシデントが発生した際にも、流出・毀損したデータの特定や原因究明のための作業を実施できる管理ツールが提供されていることを確認した。
A38730002	運109	V. 運用基準	クラウドサービスの利用	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。	安全性確保のため、機密保護、安定的なシステム運用等に関する項目を盛り込んだ契約を締結すること。	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	(1) システム運用(可用性(注)、信頼性、性能、拡張性、稼働時間、ネットワークを含む管理体制)の保証 (注) システム運用の可用性に関する指標の評価にあたっては、以下のような事項を考慮する必要がある。 1) 障害等に伴うシステムの停止時間 2) システムの更新・保守(緊急的なセキュリティパッチ対応を含む)や新サービスの追加などシステムの品質・セキュリティ向上のための計画停止期間 なお、上記2)に関して、グローバルベースでサービスが提供されるパブリッククラウドでは、緊急的なセキュリティ対策等に係る計画停止作業について、ユーザー全体の安定性を優先するため、必ずしも個々のユーザーの要望(作業のタイミングや時間等)に沿わない形で実施される可能性があることにも留意する必要がある。	○	○	5、21、24	AWSは、サービスレベルアグリーメント(SLA)で高レベルの可用性を提供しています。例えば、Amazon EC2 は、1 年のサービス期間で 99.95% 以上の稼働時間となっています。Amazon S3 は毎月 99.9% 以上の稼働時間です。こうした可用性の評価指標が基準に満たない場合は、サービスクレジットが提供されます。	簡易な管理が求められる場合には、標準的約款のカスタマイズは必須でなく、AWS標準のカスタマーアグリーメント、各種SLAですぐにでもAWSが利用可であることを確認した。 厳格な管理が求められる場合には、各金融機関のセキュリティポリシーに合わせクラウド事業者が提供する標準的約款をカスタマイズしリスク管理に必要な事項を業務委託契約、SLA/SLOに盛り込む必要がある。
							(2) サポート(障害対応、問合せ対応)の保証			21 、22	—	
							(3) データ管理の保証(利用者データの保証)			5、21	—	
							(4) 統制環境(再委託先管理(再々以下の階層の先を含む)、機密保護の維持、統制環境の維持)の保証			5、21	—	
A38730003	運109	V. 運用基準	クラウドサービスの利用	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。	安全性確保のため、機密保護、安定的なシステム運用等に関する項目を盛り込んだ契約を締結すること。	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。		—	○	N/A(利用者側対応事項)	—	—
A38730004	運109	V. 運用基準	クラウドサービスの利用	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。	安全性確保のため、機密保護、安定的なシステム運用等に関する項目を盛り込んだ契約を締結すること。	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	(1) クラウド事業者による移行すべきデータの抽出方法の提供及び移行作業への協力義務に関する契約書への明記	○	○	5、21	お客様は、お客様のデータの統制と所有権を保持します。AWS では、必要に応じてお客様がデータをAWSストレージから出し入れすることを許可しています。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を許可しています。ただし、AWSではテープへのバックアップサービスを提供していません。	簡易な管理が求められる場合には、クラウド事業者の協力を前提とせず、別のクラウド事業者に移行するための準備をあらかじめ行なっておくことをもって代替することが可能であることを確認した。 公開文書によりAWSの提供するIaaSでは、クラウド事業者の協力がなくても比較的容易に別のクラウドサービスに移行することが可能であることを確認した。 厳格な管理が求められる場合には、クラウド事業者によるデータ抽出方法の提供及び移行作業への協力義務やシステム移行作業にかかる費用負担の契約書への明記が必要となる。公開文書によりAWSではデータの所有権は金融機関に帰属し契約解除後のデータ取り出しの支援が明記されていることを確認した。 各金融機関の個別の要望については、相談が可能であることを確認した
							(2) 契約の解約時におけるシステム移行作業にかかる費用負担の契約書への明記 ただし、金融機関等において業務の特性を十分検討したうえで、委託する業務の重要度が高くないと判断し得る場合は、クラウド事業者の協力を前提とせず、別のクラウド事業者に移行するための準備をあらかじめ行っておくことをもって代替することが可能である。例えば、コンピューティング資源のみを委託するIaaS(Infrastructure as a Service)の場合では、クラウド事業者の協力がなくても比較的容易に別のクラウドサービス基盤に移行することが可能であるため、こうしたケースに該当すると考えられる。			5、21	—	
A38740001	運110	V. 運用基準	クラウドサービスの利用	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。	ファイルのコピーや盗難等による漏洩を防止するため、重要なデータについては暗号化等の対策を講ずること。	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。	(1) 蓄積・伝送データの暗号化 機密性の高い個人データ等が含まれているデータについては、暗号化等の管理策を講じることが必要である。 なお、仕様上の制約から暗号化が不可能な部分(平文で処理される部分)でのデータ覗き見リスクを把握するため、暗号化の仕様(処理プロセスにおいてどの部分が暗号化されておりどの部分がされていないか、暗号方式、暗号鍵の管理態勢等)を把握し、自社のリスク管理のポリシーに合致しているかどうか判断する必要がある。	○	○	5	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。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は、AWSインフラストラクチャ内で採用される必要な暗号化用の暗号キーを内部的に確立、管理しています。AWSはNISTで承認されたキー管理テクノロジーとプロセスをAWS情報システムで使用して対称暗号キーを作成、管理、配布しています。対称キーの作成、保護、配布には、AWSが開発したセキュアキーおよび認証情報マネージャーが使用され、ホストで必要なAWS認証情報、RSAパブリック/プライベートキー、およびX.509認証をセキュリティ保護、配布するために使用されます。AWS暗号化プロセスは、SOC、PCI DSS、ISO 27001、およびFedRAMPsm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。AWS CloudHSMサービスにより、安全なキー管理に対する米国政府標準規格に適合するように設計/検証されたHSM内で暗号キーを保護することができるようになります。データ暗号化に使用される暗号キーを安全に生成、保存、管理することで、ユーザーだけが暗号キーにアクセスできるようになります。AWS CloudHSMにより、アプリケーションのパフォーマンスを低下させることなく、厳密なキー管理要件に準拠することができます。AWS CloudHSMサービスはAmazon Virtual Private Cloud (VPC)と共に動作します。CloudHSMは指定したIPアドレスでVPC内にプロビジョニングされます。これにより、Amazon Elastic Compute Cloud (EC2)インスタンスに対して簡単でプライベートなネットワーク接続が可能になります。CloudHSMをEC2インスタンス近くに配置することで、ネットワークレイテンシーは低減され、アプリケーションのパフォーマンスが向上します。AWSにはCloudHSMへの専用かつ排他的アクセスが用意されており、他のAWSのユーザーとは分離されています。AWS CloudHSMは複数のリージョンとアベイラビリティーゾーン(AZ) で利用でき、Amazon EC2アプリケーションに対して安全で耐久性の高いキーストレージを追加することができます。	重要データを扱わない場合には、暗号化等の管理策は省略でき、また機密性の高いデータについては、公開文書によりデータ漏洩防止策として、ほぼ全てのサービスで金融機関独自の暗号化メカニズムの使用が許可されていることを確認した。 暗号鍵の管理機能(CloudHSM)の利用により、金融機関で暗号鍵を管理することが可能であることを確認した。 蓄積・伝送データの暗号化対策においても十分な強度を持った方式が利用できることを確認した。
							(2) 暗号鍵の管理主体 クラウド事業者に暗号鍵の管理を委ねる場合には、その管理策の概要を十分に把握し、自社のリスク管理のポリシーに合致していることを判断する必要がある。【運43】			—	—	
							(3) 暗号化の代替策 暗号化の代替策として、元データとトークンを金融機関側で持ち、クラウド環境下にあるデータを無作為な乱数に置き換え、実質的に無意味化するとしたトークン化技術を利用することが可能である。ただし、トークン化を管理策として採用する場合には、金融機関におけるトークンマッピング(対応表)の管理についても相応の管理策が必要となる。			—	—	
A38740002	運110	V. 運用基準	クラウドサービスの利用	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。	ファイルのコピーや盗難等による漏洩を防止するため、重要なデータについては暗号化等の対策を講ずること。	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。	(1) 交換された元の記憶装置等において実際にデータが格納されていた可能性のある記憶媒体上のデータの物理的または論理的消去を実施する(回転部や論理回路等の機器故障により論理的消去の操作ができない場合は、物理的消去を実施)	○	○	5	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。	重要データを扱わない場合には、記憶装置の交換に際し、データの消去・破壊を実施しないことも可能であることを確認した。 AWSはストレージデバイスが耐用年数の終わりに達した際の顧客データ流出防止のための廃棄プロセスの一環としてデータ破壊を行ない、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、物理的に破壊する手順を公開文書で確認した。またこのプロセスが第三者監査の対象となっていることをNDA情報により確認した。 またAWSは記憶装置の故障等による交換の際にも、上記耐用年数終了時の顧客データ流出防止のための廃棄プロセスを同様に実施していることをインタービューにより確認した。
							(2) クラウド事業者の施設外に搬出される前に物理的消去を実施する			—	—	
							(3) 復元を不可能または著しく困難な状態にしたうえで持ち出すといった点をあらかじめ契約書またはSLA等に明記する			—	—	
							(4) データの消去の方法として、必要に応じて【運75】も参照のこと。 ただし、重要なデータを扱わない場合は、記憶装置等の交換に際し、データの消去・破壊を実施しないことも可能である。			—	—	

FISC 安全対策基準第8版および第8版追補改訂からの引用								対応の主体		対応可否判断のための情報参照元	AWSの該当情報	確認した内容と解説
	項番	基準大項目	基準中項目	基準小項目	適用にあたっての考え方	基準項目の目的 内容説明 具体例等の解説	基準項目の目的 内容説明 具体例等の解説	クラウド事業	利用者	基準項目に対するクラウド事業者の一般公開情報の所在		
A38750001	運111	V. 運用基準	クラウドサービスの利用	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。	機密保護や不正防止等のため、クラウド契約の終了にあたっては当該システム・機器等からデータの漏洩が生じないように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78】		○	○	5	AWSは、お客様に対して、お客様のデータを削除する機能を提供しています。ただし、AWSのお客様は、お客様のデータの統制と所有権を有していますので、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はお客様のプライバシー保護を慎重に考慮し、AWSが準拠する必要がある法的処置の要求についても注意深く判断しています。AWSは、法的処置による命令に確実な根拠がないと判断した場合は、その命令にたからわずに異議を申し立てます。	重要データを扱わない場合には、契約終了時のデータの消去プロセスを簡略化または不要とし、消去証明書を不要とすることも可能であり、また消去プロセスの実施を契約書に明記し、かつ外部の第三者監査等で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・取得の代替も可能であることを確認した。 AWSはストレージデバイスが耐用年数の終わりに達した際の顧客データ流出防止のための廃棄プロセスの一環としてデータ破壊を行ない、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、物理的に破壊する手順を公開文書で確認した。またこのプロセスが第三者監査の対象となっていることをNDA情報により確認した。
A38750002	運111	V. 運用基準	クラウドサービスの利用	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。	機密保護や不正防止等のため、クラウド契約の終了にあたっては当該システム・機器等からデータの漏洩が生じないように防止策を講ずること。	2. データ消去にあたっては、以下の方法が考えられる。	(1) 物理的消去(消磁や破壊)	○	○	5	AWSは、お客様に対して、お客様のデータを削除する機能を提供しています。ただし、AWSのお客様は、お客様のデータの統制と所有権を有していますので、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) 以下のいずれかによる論理的消去 1) データ管理領域とデータ保存領域のリンク情報を不可逆的に切断すること 2) 全データの保存領域を、意図的に無意味なデータまたは他のユーザのデータにより上書きすること 3) 保管データが暗号化されている場合には、暗号鍵を廃棄すること なお、将来的なハードウェア更改・撤去時に物理的消去を行うことが望ましい。			―	―	
A38750003	運111	V. 運用基準	クラウドサービスの利用	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。	機密保護や不正防止等のため、クラウド契約の終了にあたっては当該システム・機器等からデータの漏洩が生じないように防止策を講ずること。	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。		—	○	5	AWSは、お客様に対して、お客様のデータを削除する機能を提供しています。ただし、AWSのお客様は、お客様のデータの統制と所有権を有していますので、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。	
A38750004	運111	V. 運用基準	クラウドサービスの利用	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。	機密保護や不正防止等のため、クラウド契約の終了にあたっては当該システム・機器等からデータの漏洩が生じないように防止策を講ずること。	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。		—	○	5	AWSは、お客様に対して、お客様のデータを削除する機能を提供しています。ただし、AWSのお客様は、お客様のデータの統制と所有権を有していますので、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。	
A38760001	運112	V. 運用基準	クラウドサービスの利用	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。	直接の内部統制の及びにくいクラウド事業者について、リスク管理態勢等の有効性を検証すること。	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。	-	○	○	5	従来、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います。お客様またはお客様の社外監査人による直接の監視または検証は、一般的に、統制の妥当性を確認するために行われます。AWS などのサービスプロバイダを使用する場合、企業はサードパーティによる証明および認定を要求し、評価することで、統制目標と統制の設計と運用効率の合理的な保証を獲得します。その結果、お客様の主な統制を AWS が管理している場合でも、統制環境を統一されたフレームワークの主要機能し、効率的に運用しながらすべての統制を把握し、検証することができます。サードパーティによる証明と AWS の認定によって、統制環境を高いレベルで検証できるだけでなく、AWS クラウドの自社の IT 環境に対して特定の検証作業を自社で実行する要求を持つお客様にも役立ちます。	簡易な管理が求められる場合には、立入監査の代替として以下がある。 (1)ISO27001、SOC2、PCIDSS level1他の第3者認証レポートの活用。 (2)セキュリティに係るホワイトペーパーの確認、レビュー (3)リスク管理に必要なデータ抽出ツールの提供 AWSは公開文書としてセキュリティに関するホワイトペーパーを提供。 またNDA締結により、SOC1,2、ISO27001、PCIDSSを閲覧可能であることを確認した。
A38760002	運112	V. 運用基準	クラウドサービスの利用	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。	直接の内部統制の及びにくいクラウド事業者について、リスク管理態勢等の有効性を検証すること。	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。	-	○	○	5	ほとんどのレイヤーと、物理統制よりも上の統制の監査は、お客様の担当です。AWS 定義の論理統制と物理統制の定義は、SOC 1 Type II レポート（SSAE 16）に文書化されています。また、このレポートは、この監査チームとコンプライアンスチームのレビューに使用できます。また、AWS ISO 27001 およびその他の認定も、監査人のレビュー用に使用できます。 AWS は外部の認定機関および独立監査人と協力し、AWS が制定・運用するポリシー、プロセス、および統制に関する重要な情報をお客様に提供しています。 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、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、FedRAMPsm テストプログラムの一部となっています。	
A38760003	運112	V. 運用基準	クラウドサービスの利用	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。	直接の内部統制の及びにくいクラウド事業者について、リスク管理態勢等の有効性を検証すること。	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。	(1) 検証項目については、クラウドのリスクプロファイルを踏まえた検証、委託元金融機関の検証ニーズに則った検証を行うこと。 なお、委託元金融機関が単独、または他の金融機関と共同で第三者監査人と監査契約を締結し、クラウド事業者に対する監査を行う場合、既にクラウド事業者が受検している監査結果の内容を検証し、疑問点や不足する監査項目を中心にクラウド事業者に対する実地検証を行うことが有効である。	○	○	5	AWS は、サードパーティによる証明、認定、Service Organization Controls 1 (SOC 1) Type II レポートなどの関連するコンプライアンスレポートを、NDA に従ってお客様に直接提供しています。 AWS セキュリティは、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。	
							(2) 委託元金融機関が、単独または共同で第三者監査人とクラウド事業者に対する監査に関する契約を締結し、クラウド事業者に対する監査を行う体制も選択可能とすること。			2、5、8	―	
							(3) 委託元金融機関側が、第三者監査に関する費用を負担(または分担)する体制に移行すること。			―	―	
							(4) 同一の監査責任者が長期間にわたり監査を行うことによる外観的独立性に対する疑念を払拭するため、適切なサイクルで交代すること。			―	―	
							(5) 監査の品質を引き上げるために、SOC2等、監査人側の損害賠償責任が契約書上明確化されている監査スキームを活用すること。			2、5	―	
							(6) 第三者監査人の適格性の担保のため、監査人(監査法人)が日本公認会計士協会等の指導や指針等に基づいて、適切な品質管理体制の整備、運用を実施すること。			―	―	
							(7) 第三者監査を効率的に行うため、複数の委託元金融機関が共同で第三者に監査実施を委託すること。			2、5	―	
							(8) 海外でのデータ保管時において、当該データセンターへの往査に必要な時間やコスト等を考慮すること。			7	―	
A38760004	運112	V. 運用基準	クラウドサービスの利用	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。	直接の内部統制の及びにくいクラウド事業者について、リスク管理態勢等の有効性を検証すること。	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。	(1) その業務の必要とする立入監査等の項目をカバーし、内容が十分と判断できる第三者認証(注)のレポートの活用 (注) 各国の公認会計士協会や業界団体等が定める事業者等の情報セキュリティ体制やプライバシー保護体制の基準等に係る認証。代表的なものとして、ISMS(ISO27001)やPCI DSS level1、SOC1、SOC2、監査・保証実務委員会実務指針第86号、IT委員会実務指針7号、プライバシーマーク等がある。	○	○	2、5	AWSでは、AWS は外部の認定機関および独立監査人と協力し、AWS が制定・運用するポリシー、プロセス、および統制に関する重要な情報をお客様に提供しています。(ISO27001、PCI DSS v3.1、SOC1、SOC2、SOC3など)	
							(2) クラウド事業者が準備するセキュリティに係るホワイトペーパーの確認またはレビュー			1	―	
							(3) リスク管理に必要なデータ抽出のツールをクラウド事業者側から準備・提供する			6	―	

FISC 安全対策基準第8版および第8版追補改訂からの引用								対応の主体		対応可否判断のための情報参照元	AWSの該当情報	確認した内容と解説
項番	基準大項目	基準中項目	基準小項目	適用にあたっての考え方	基準項目の目的　内容説明　具体例等の解説	基準項目の目的　内容説明　具体例等の解説		クラウド事業	利用者	基準項目に対するクラウド事業者の一般公開情報の所在		
運113	V.　運用基準	サイバー攻撃対応態勢の整備	運113　サイバー攻撃対応態勢を整備すること。	サイバー攻撃の手口は高度化かつ巧妙化しているため、サイバー攻撃対応態勢の整備にあたっては、手口の高度化や巧妙化にあわせて見直すことが必要である。	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。			○	○	5	AWSセキュリティは、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。これらのスキャンは、基礎となる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のものであり、顧客固有のコンプライアンス要件に適合する必要のある、顧客自身の脆弱性スキャンに置き換えることを意味するものではありません。お客様は事前に承認を得た上で、お使いのクラウドインフラストラクチャにスキャンを実施することができます。対象はお客様のインスタンスに限り、かつAWS利用規約に違反しない範囲とします。このようなスキャンについて事前に承認を受ける必要はは、AWS脆弱性/侵入テストリクエストフォームを使用してリクエストを送信してください。	公開文書により、AWSではインシデント対応組織等が明記されている事を確認した。金融機関がAWS上で構築する環境については、金融機関のサイバーセキュリティ等の運用に則り対策を検討する必要がある。
運113	V.　運用基準	サイバー攻撃対応態勢の整備	運113　サイバー攻撃対応態勢を整備すること。	サイバー攻撃の手口は高度化かつ巧妙化しているため、サイバー攻撃対応態勢の整備にあたっては、手口の高度化や巧妙化にあわせて見直すことが必要である。	2.　未然防止策・事前対策には、以下のような例がある。	(1) 外部の第三者によるセキュリティ評価を行うこと。不正侵入防止における評価については【技43】を参照のこと。		○	○	1　侵入テスト		金融機関側で客観的評価に必要な情報がAWSから提供される事を確認した。金融機関はペネトレーションテストを実施する前に、AWSに申請する必要がある。
						(2) 業務委託先、業務提携先等のうち、重要な関係先のサイバー攻撃対応態勢の整備状況を確認すること。特に、外部委託先に対するサイバー攻撃対応態勢の整備状況確認については、監査の一環として行うことが有効であるため、【運88】【運90】【運91】を参照のこと。		○	○	5		公開文書により、AWSのインシデント対応ポリシー等が明記されていることを確認した。
						(3) インシデント発生時における部署間の連携や、外部との連絡窓口の機能を担い、経営陣への報告並びに経営陣からの指示を実施することができる組織を整備すること。例としてCSIRT(Computer Security Incident Response Team)の設置等がある。【技43】(参考4)		○	○	5		公開文書により、AWSではインシデント対応組織等が明記されている事を確認した。金融機関がAWS上で構築する環境については、金融機関のサイバーセキュリティ等の運用に則り対策を検討する必要がある。
						(4) 大規模な攻撃が行われた場合も含め、サイバー攻撃発生時の外部ベンダー等のフォレンジックなどに関するサービス提供能力を把握すること。		○	○	20		公開文書により、AWSのDDoS攻撃を緩和する方法を確認した。
						(5) 顧客が必要とする機能、並びに利用環境やITリテラシー等のセキュリティレベルを踏まえて、利用可能な機能や限度額を設定すること。取引制限については【技30】を参照のこと。		—	○	N/A（利用者側対応事項）	—	—
						(6) インターネット取引を求める顧客に対し、不正プログラム対策ソフトの導入有無等、利用者が利用するパソコン環境の事前告知を求めること。		—	○	N/A（利用者側対応事項）	—	—
運113	V.　運用基準	サイバー攻撃対応態勢の整備	運113　サイバー攻撃対応態勢を整備すること。	サイバー攻撃の手口は高度化かつ巧妙化しているため、サイバー攻撃対応態勢の整備にあたっては、手口の高度化や巧妙化にあわせて見直すことが必要である。	3.　検知策には、以下のような例がある。	(1) インシデントレスポンス態勢を整備すること。その前提として、システム全体の監視を行うことが必要となるため、【運60】を参照のこと。		○	○	—	AWSは、様々な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。AWSモニタリングツールは、異常な、または不正なアクティビティと条件を通信の出入りロで検出するように設計されています。これらのツールは、サーバーおよびネットワークの利用状況、ポートスキャニングアクティビティ、アプリケーションの利用状況、および許可されていない侵入の試みをモニタリングします。このツールを使用して、異常なアクティビティに対して独自に性能測定基準のしきい値を設定することができます。	公開文書により、AWSではインシデント対応組織等が明記されている事を確認した。金融機関がAWS上で構築する環境については、金融機関のサイバーセキュリティ等の運用に則り対策を検討する必要がある。
						(2) アクセス履歴を監査すること。アクセス履歴の監査については【技37】の2.を参照のこと。		○	○	19		AWSが提供する（CloudTrail）によってアクティビティの可視化が可能であることを確認した。
						(3) 不正アクセス監視の一環として、侵入検知システム等による自動監視等、ネットワークの監視を行うこと。詳細については、【技45】を参照のこと。		○	○	19		
運113	V.　運用基準	サイバー攻撃対応態勢の整備	運113　サイバー攻撃対応態勢を整備すること。	サイバー攻撃の手口は高度化かつ巧妙化しているため、サイバー攻撃対応態勢の整備にあたっては、手口の高度化や巧妙化にあわせて見直すことが必要である。	4.　対応策には、以下のような例がある。	(1) サイバー攻撃の発生直後はシステム障害と区別ができない可能性も想定されるため、システム障害時にサイバー攻撃の可能性を考慮すること。システム障害時の対応手順の整備については【運63】、連絡手順については【運62】を参照のこと。		○	○	—	インシデント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。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。	AWSが提供する（CloudTrail）によってアクティビティの可視化が可能。金融機関がAWS上で構築する環境については、金融機関のサイバーセキュリティ等の運用に則り対策を検討する事が必要であることを確認した。
						(2) 利用者(顧客)への説明を行うこと。顧客への対応方針については、【運105-1】を参照のこと。		—	○	N/A（利用者側対応事項）		—
						(3) システムの全部または一部を、一時的に停止すること。不正アクセスの拡大防止については、【技48】を参照のこと。		○	○	5		金融機関がAWS上で構築する環境については、金融機関のサイバーセキュリティ等の運用に則り対策を講じる必要がある。
						(4) 侵入経路及び手口、情報流出の痕跡及び範囲などを分析するフォレンジックを実施すること。ただし、サイバー攻撃の高度化及び複雑化に伴い、フォレンジックに必要なデータの取得対象、範囲及び期間並びに事象発生時の証拠保全方法は変化することから、実施にあたっては、専門的な知識や技術を持つ外部業者に委託することも有効である。		○	○	18		AWSが提供する（CloudTrail）によってトレーサビリティ確保のための各種ログの取得が可能。金融機関がAWS上に構築する環境においては必要なログ取得は金融機関にて管理する必要がある。
運113	V.　運用基準	サイバー攻撃対応態勢の整備	運113　サイバー攻撃対応態勢を整備すること。	サイバー攻撃の手口は高度化かつ巧妙化しているため、サイバー攻撃対応態勢の整備にあたっては、手口の高度化や巧妙化にあわせて見直すことが必要である。	5.　教育・訓練には、以下のような例がある。	(1) サイバー攻撃を想定した対応訓練を実施すること。		○	○	5	ISO27001基準に合わせて、すべてのAWS従業員は、修了時に承認を必須とする定期的な情報セキュリティトレーニングを修了しています。作成したポリシーを従業員が理解し、従っていることを検証するために、コンプライアンス監査が定期的に実施されます。	公開文書により、AWSのセキュリティトレーニングが明記されている事を確認した。金融機関がAWS上で構築する環境については、金融機関のサイバーセキュリティ等の運用に則り対策を検討する必要がある。
						(2) サイバー攻撃対応の意識を高めるためにも、データやファイル交換を行う当事者同士が必要に応じて相互のサイバー攻撃対応態勢について確認すること。		○	○	5		
						(3) 教育・訓練の実施に際しては、コンピュータセンターと本部・営業店等との連携を行うこと。また、業界団体が訓練を開催する場合には参加すること。		○	○	5		
						(4) サイバー攻撃を受けるリスクや、受けた場合の対応手順は、関係する役職員、外部委託先に対して周知、啓発を行い、訓練を実施すること。関係する役職員に対しては【運80】、外部委託先に対しては【運89】をそれぞれ参照のこと。		○	○	5		
						(5) 顧客に対して、サイバー攻撃を受けるリスクや防止策を周知し、注意喚起を行うこと。注意喚起すべき内容については【運105-1】を参照のこと。		—	○	N/A（利用者側対応事項）	—	—
運113	V.　運用基準	サイバー攻撃対応態勢の整備	運113　サイバー攻撃対応態勢を整備すること。	サイバー攻撃の手口は高度化かつ巧妙化しているため、サイバー攻撃対応態勢の整備にあたっては、手口の高度化や巧妙化にあわせて見直すことが必要である。	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。			—	○	N/A（利用者側対応事項）	—	金融機関がAWS上で構築する環境については、金融機関のサイバーセキュリティ等の運用に則り対策を検討必要がある。また、情報共有機関や外部サービスを利用する事により、サイバー攻撃発生時の対応体制を構築する事も可能であることを確認した。

記号	情報源名称	参照先
1	AWS セキュリティセンター	https://aws.amazon.com/jp/security/
2	AWS コンプライアンス	https://aws.amazon.com/jp/compliance/
3	ガートナー他のアナリストレポート	https://aws.amazon.com/jp/resources/analyst-reports/
4	国内のお客様の導入事例	http://aws.amazon.com/jp/solutions/case-studies-jp/
5	アマゾン ウェブ サービス:リスクおよびコンプライアンス	https://s3.amazonaws.com/awsmedia/jp/wp/AWS_Risk_and_Compliance_Whitepaper.pdf
6	Security at Scale: Logging in AWS	http://d0.awsstatic.com/whitepapers/compliance/AWS_Security_at_Scale_Logging_in_AWS_Whitepaper.pdf
7	AWS Security Best Practices	https://d0.awsstatic.com/whitepapers/aws-security-best-practices.pdf
8	AWS エンタープライズプロフェッショナルサービス	https://aws.amazon.com/jp/professional-services/
9	Amazon Web Services：セキュリティプロセスの概要	http://media.amazonwebservices.com/jp/wp/AWS_Security_Whitepaper_JP_201505.pdf
10	金融機関におけるクラウド利用に関する有識者検討会報告書	https://www.fisc.or.jp/
11	AMAZON 2014 Annual Report	https://www.sec.gov/Archives/edgar/data/1018724/000101872415000006/amzn-20141231x10k.htm
12	SOC 1 Type II レポート	https://aws.amazon.com/jp/compliance/soc-faqs/
13	SOC 2 監査レポート	https://aws.amazon.com/jp/compliance/soc-faqs/
14	SOC 3 監査レポート	https://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf
15	Introduction to AWS Securit	https://d0.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf
16	AWS セキュリティのベストプラクティス	http://media.amazonwebservices.com/jp/wp/AWS_Security_Best_Practices.pdf
17	アマゾンウェブサービスの概要	https://media.amazonwebservices.com/jp/wp/AWS_Overview.pdf
18	PCD DSS Level 1に対するFAQ	https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/
19	CloudTrail	https://aws.amazon.com/jp/cloudtrail/
20	ホワイトペーパー DDoSに対するAWSのベストプラクティス	http://media.amazonwebservices.com/jp/DDoS%20White%20Paper_Revised.pdf
21	AWS カスタマーアグリーメント	https://aws.amazon.com/jp/agreement/
22	AWS サポート	https://aws.amazon.com/jp/premiumsupport/
23	責任共有モデル	https://aws.amazon.com/jp/compliance/shared-responsibility-model/
24	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/
25	「Enterprise Agreement」に関する公開情報	https://aws.amazon.com/pricing/enterprise/

※参照元は各社が確認を行った時点のもので、ご利用時に参照できないあるいは内容が変更となっている場合がある。