金融機関等コンピュータシステムの安全対策基準 第8版

***Amazon Web Services* の回答　*2012*年*6*月**

基準大項目	中項目	項番	小項目	AWS回答
建物	**環境**	設1	各種災害、障害が発生しやすい地域を避けること。	AWSのデータセンターは、革新的なデザインと工学的なアプローチを活用し、環境的なリスクに対して、物理的な保護を行なっています。 追加情報については、"AWSのセキュリティ･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 さらに、ISO 27001の附属書 A. 9.1もしくは SOC1タイプ2レポートで詳細を提供しています。 AWSは独立した監査人によって検証され、ISO 27001認証への準拠が確認されています。
	周囲	設2	立地環境の変化に伴う災害および障害の発生の可能性を調査し、防止対策を講ずること。	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。物理的なセキュリティ対策としては、フェンス、壁、セキュリティスタッフ、監視カメラ、侵入検知システムやその他エレクトロニクスを用いた厳重な管理を行っています。 AWS SOC1 タイプ2レポートに、AWS特有の取り組みに関するさらなる詳細情報が記載されています。 追加の情報についてはISO27001 附属書 A. 9.1をご参照ください。AWSは独立した監査人によって検証され、ISO 27001認証への準拠が確認されています。
		設3	敷地には通路を確保すること。	
		設4	隣接物との間隔を十分に取ること。	
		設5	塀または柵および侵入防止装置を設けること。	
		設6	看板等を外部に出さないこと。	
		設7	建物には避雷設備を設置すること。	
		設8	建物はコンピュータシステム関連業務専用、または建物内においてコンピュータシステム関連業務専用の独立区画とすること。	
		設9	敷地内の通信回線・電力線は、切断・延焼の防止措置を講ずること。	
	構造	設10	耐火建築物であること。	AWSのデータセンターは環境的なリスクに対する物理的な保護を備えています。AWSの環境的なリスクに対する物理的な保護は、独立した監査人によって検証され、ISO27002のベストプラクティスに準拠することが承認されています。 詳細についてはISO27001 附属書 A. 9.1、AWS SOC1 タイプ2レポートを参照してください。
		設11	構造の安全性を有すること。	
		設12	外壁、屋根等は十分な防水性能を有すること。	
		設13	外壁等に強度を持たせること。	
	開口部	設14	窓には防火措置を講ずること。	物理的なセキュリティ対策としては、フェンス、壁、セキュリティスタッフ、監視カメラ、侵入検知システムやその他エレクトロニクスを含む手段を用いて厳重な管理を行っています。
		設15	防犯措置を講ずること。	

基準大項目	中項目	項番	小項目	AWS回答
		設16	常時利用する出入口は1カ所とし、出入管理設備、防犯設備を設置すること。	AWS SOC1 タイプ2レポートに、AWSにおける取り組みに関するさらなる詳細情報が記載されています。 追加の情報についてはISO27001 附属書 A. 9.1を参照してください。AWSは独立した監査人によって検証され、ISO 27001認証に準拠することが確認されています。
		設17	非常口を設けること。	
		設18	防水措置を講ずること。	
		設19	出入口の扉は、十分な強度を持たせるとともに、錠を付けること。	
	内装等	設20	不燃材料および防炎性能を有するものを使用すること。	AWSのデータセンターは環境的なリスクに対する物理的な保護を備えています。AWSの環境的なリスクに対する物理的な保護は、独立した監査人によって検証され、ISO27002のベストプラクティスに準拠することが承認されています。 詳細についてはISO27001 附属書 A. 9.1、AWS SOC1 タイプ2レポートを参照してください。
		設21	地震による内装等の落下・損壊の防止措置を講ずること。	
コンピュータ室・データ保管室	**位置**	設22	災害を受けるおそれの少ない位置に設置すること。	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。AWSのデータセンターは環境的なリスクに対する物理的な保護を備えています。 追加情報に関しては下記の「Amazon Web Servicesセキュリティプロセス概要」白書をご参照ください。 http://aws.amazon.com/security また、ISO27001 附属書 A. 9.1、AWS SOC1 タイプ2レポートにさらなる詳細が記載されています。AWSは独立した監査人によって検証され、ISO 27001認証に準拠することが確認されています。
		設23	外部から容易に入れない位置に設置すること。	
		設24	室名等の表示は付さないこと。	
		設25	必要空間を確保すること。	
		設26	専用の独立した室とすること。	
	開口部	設27	常時利用する出入口は1カ所とし、前室を設けること。	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。物理的なセキュリティ対策としては、フェンス、壁、セキュリティスタッフ、監視カメラ、侵入検知システムやその他エレクトロニクスを用いた厳重な管理を行っています（但し、
		設28	出入口の扉は、十分な強度を持たせるとともに、錠を付けること	

基準大項目	中項目	項番	小項目	AWS回答
		設29	窓に防火、防水、破損防止措置を講じ、外部から室内の機器等が見えない措置を講ずること。	手段はこの限りではない）。 AWS SOC1 タイプ2レポートに、AWS特有の取り組みに関するさらなる詳細情報が記載されています。 追加の情報についてはISO27001 附属書 A. 9.1をご参照ください。AWSは独立した監査人によって検証され、ISO 27001認証への準拠が確認されています。
		設30	非常口、避難器具、誘導灯等を設置すること。	
	構造・内装等	設31	独立した防火区画とすること。	AWSのデータセンターは環境的なリスクに対する物理的な保護を備えています。 追加情報に関しては下記の「Amazon Web Servicesセキュリティプロセス概要」白書をご参照ください。 http://aws.amazon.com/security また、ISO27001 附属書 A. 9.1、AWS SOC1 タイプ2レポートにさらなる詳細が記載されています。AWSは独立した監査人によって検証され、ISO 27001認証に準拠することが確認されています。
		設32	漏水防止対策を講ずること。	
		設33	静電気の防止措置を講ずること。	
		設34	内装等には不燃材料および防炎性能を有するものを使用すること。	
		設35	地震による内装等の落下・損壊の防止措置を講ずること。	
		設36	フリーアクセス床は地震時に損壊しない構造とすること。	
	設備	設37	自動火災報知設備を設置すること。	AWSのデータセンターは環境及びセキュリティに関するリスクに対する物理的な保護を備えています。これには、火気の検知と抑制、空気のコンディションを最適なレベルに調整する空調、物理的なセキュリティ制御などが含まれます。 追加情報に関しては下記の「Amazon Web Servicesセキュリティプロセス概要」白書をご参照ください。 http://aws.amazon.com/security また、ISO27001 附属書 A. 9.1、AWS SOC1 タイプ2レポートにさらなる詳細が記載されています。AWSは独立した監査人によって検証され、ISO 27001認証に準拠することが確認されています。
		設38	非常時の連絡装置を設置すること。	
		設39	消火設備を設置すること。	
		設40	ケーブルの難燃化、延焼防止措置を講ずること。	
		設41	排煙設備を設置すること。	
		設42	非常用照明設備、携帯用照明器具を設置すること。	
		設43	水使用設備を設置しないこと。	
		設44	地震感知器を設置すること。	
		設45	出入口には出入管理設備、防犯設備を設置すること。	
		設46	温湿度自動記録装置または温湿度警報装置を設置すること。	
		設47	ネズミの害を防止する措置を講ずること。	
	コンピュータ機器、	設48	什器・備品は不燃性とすること。	AWSのデータセンターは地震を含む局所的な環境リスクに対する警報と物理的な保護を備えています。

基準大項目	中項目	項番	小項目	AWS回答
	什器・備品	設49	静電気防止措置を講ずること。	追加情報に関しては下記の「Amazon Web Servicesセキュリティプロセス概要」白書をご参照ください。 http://aws.amazon.com/security
		設50	耐震措置を講ずること。	
		設51	運搬車等に固定装置を取り付けること。	
電源室・空調機械室		設52	災害を受けるおそれの少ない場所に設置すること。	AWSのデータセンターは環境リスクに対する物理的な保護を備えています。これには、火気の検知と抑制、空気のコンディションを最適なレベルに調整する空調、完全に冗長化された電源システムなどが含まれます。物理的なセキュリティ対策としては、フェンス、壁、セキュリティスタッフ、監視カメラ、侵入検知システムやその他エレクトロニクスを使った手段を含む制限を行っています。 追加情報に関しては「Amazon Web Servicesセキュリティプロセス概要」のホワイトペーパーを参照して下さい。 http://aws.amazon.com/security また、ISO27001 附属書 A. 9.1、AWS SOC1タイプ2レポートにさらなる詳細が記載されています。AWSは独立した監査人によって検証され、ISO 27001認証に準拠することが確認されています。
		設53	保守点検に必要な空間を確保すること。	
		設54	専用の独立した室とすること。	
		設55	無窓とし、錠を付けた扉を設置すること。	
		設56	耐火構造とすること。	
		設57	自動火災報知設備を設置すること。	
		設58	ガス系消火設備を設置すること。	
		設59	空調設備の漏水防止措置を講ずること。	
		設60	ケーブル、ダクトからの延焼防止措置を講ずること。	
電源設備		設61	電源設備の容量には余裕を持たせること。	データセンターの電力システムは、完全に冗長性をもち、1日24時間・週7日、運用に影響を与えることなくメンテナンス可能な設計がなされています。施設内の重要かつ不可欠な箇所における電力障害に際しては、無停電電源装置（UPS）がバックアップ電力を供給します。データセンターは、施設全体へのバックアップ電力を供給する発電機を備えています。 追加情報に関しては「Amazon Web Servicesセキュリティプロセス概要」のホワイトペーパーを参照して下さい。 http://aws.amazon.com/security また、ISO27001 附属書 A. 9.1、AWS SOC1タイプ2レポートにさらなる詳細が記載されています。AWSは独立した監査人によって検証され、ISO 27001規格に準拠することが確認されています。
		設62	電源は複数回線で引き込むこと。	
		設63	良質な電力を供給する設備を設置すること。	
		設64	自家発電設備、蓄電池設備を設置すること。	
		設65	電源設備には避雷設備を設置すること。	
		設66	電源設備には耐震措置を講ずること。	
		設67	分電盤からコンピュータ機器への電源の引込みは専用とすること。	
		設68	負荷変動の激しい機器との共用を避けること。	
		設69	コンピュータシステムのアースは適切に施工すること。	
		設70	過電流、漏電により各機器に障害を及ぼさないよう措置を講ずること。	
		設71	防災、防犯設備用の予備電源を設置すること。	
空調設備		設72	空調設備の能力には余裕を持たせること。	AWSのデータセンターは環境的なリスクに対する物理的な保護を備えるよう開発されています。

基準大項目	中項目	項番	小項目	AWS回答
		設73	空調設備は安定的に空気調和できる措置を講ずること。	サーバの過熱を予防し、サービスの中断の可能性を下げるためにサーバやその他のハードウェアを一定の温度に保つには、空調が必要です。データセンターは空気のコンディションを最適なレベルに保つよう、調整されています。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及び制御を実施しています。 追加の情報についてはISO27001 附属書 A. 9.1をご参照ください。 AWSは独立した監査人によって検証され、ISO 27001規格に準拠することが確認されています。
		設74	空調設備はコンピュータ室専用とすること。	
		設75	空調設備の予備を設置すること。	
		設76	空調設備には自動制御装置、異常警報装置を設置すること。	
		設77	空調設備には侵入、破壊防止対策を講ずること。	
		設78	空調設備には耐震措置を講ずること。	
		設79	空調設備の断熱材料、給排気口は不燃材料とすること。	
監視制御設備		設80	監視制御設備を設置すること。	AWSは、電気的、機械的、物理的セキュリティ及び生存監視に関するシステムと設備を監視し、如何なる問題も速やかに特定されるようにしています。 追加情報に関しては下記の「Amazon Web Servicesセキュリティプロセス概要」白書をご参照ください。 http://aws.amazon.com/security
		設81	中央管理室を設置すること。	
回線関連設備		設82	回線関連設備には錠をつけること。	物理的なセキュリティ対策としては、フェンス、壁、セキュリティスタッフ、監視カメラ、侵入検知システムやその他エレクトロニクスを含む手段を用いて厳重な管理を行っています。これには、ネットワークケーブルの適切な保護も含まれています。 AWS SOC1 タイプ2レポートに、AWSにおける取り組みに関するさらなる詳細情報が記載されています。 追加の情報についてはISO27001 附属書 A. 9.1を参照してください。AWSは独立した監査人によって検証され、ISO 27001規格に準拠することが確認されています。
		設83	回線関連設備の設置場所の表示は付さないこと。	
		設83-1	回線は、専用の配線スペースに設けること。	
管理体制の確立	**セキュリティ管理と責任の明確化**	運1	セキュリティ管理方法を具体的に定めた文書を整備すること。	ISO27001を基準とした、セキュリティに関するポリシーおよび手順は、AWSの情報セキュリティフレームワークで確立されています。 Amazonの統制された環境は、当社のトップレベルのコミットから始まります。エグゼクティブとシニアのリーダーシップは、AWSのセキュリティマネジメントを確立する上で重要な役割を果たします。 詳細についてはAWSのリスクおよびコンプライアンスホワイトペーパーを参照してください。http://aws.amazon.com/security
		運2	セキュリティ管理方法を具体的に定めた文書の評価と改訂を行うこと。	
		運3	セキュリティ管理体制を整備すること。	
		運4	システム管理体制を整備すること。	
		運5	データ管理体制を整備すること。	
		運6	ネットワーク管理体制を整備すること。	
	組織の整備	運7	防災組織を整備すること。	AWSのコンプライアンスおよびセキュリティチームは、情報セキュリティフレームワークと、COBITフレームワークに基づいたポリシーを確立しています。 AWSのセキュリティ·フレームワークは、ISO27002のベストプラクティスおよびPCI
		運8	防犯組織を整備すること。	

基準大項目	中項目	項番	小項目	AWS回答
		運9	業務組織を整備すること。	DSSを統合して構築されています。 詳細については「AWSのリスクおよびコンプライアンス」のホワイトペーパーを参照してください。
	各種規定の整備	運10	各種規定を整備すること。	AWSは、ISO27001で要求される業界団体やリスク/コンプライアンス組織、地方当局や規制当局とのコンタクトを行なっています。
	セキュリティ遵守状況の確認	運10-1	セキュリティ遵守状況を確認すること。	AWSは特定の業界の認定や独立した第三者の証明を取得し、NDA締結下でこれらのドキュメントを提供しています。
入退管理	**入退館(室)管理**	運11	資格付与および鍵の管理を行うこと。	物理的アクセスは、ビデオ監視、侵入検知システム、およびその他の電子的な手段を活用したセキュリティ専門スタッフにより、入退室時に厳密に制御されています。入室を許可されたスタッフは、入室を行なうために最低2回の2要素認証をパスする必要があります。 詳細については、"AWSのセキュリティ·プロセスの概要"のホワイトペーパーのを参照してください。http://aws.amazon.com/security. さらに、SOC1タイプ2のレポートでは、AWSによって実行される物理アクセス制御に関する詳細を提供しています。
		運12	入退館管理を行うこと。	
		運13	入退室管理を行うこと。	
運用管理	**マニュアルの整備**	運14	通常時マニュアルを整備すること。	情報システムのドキュメントは、Amazonのイントラネット·サイトを通じで、AWSの担当者が利用できるようになっています。 詳細については、http://aws.amazon.com/securityで入手できるセキュリティ·プロセスのホワイトペーパーのAWSの概要を参照してください。 AWSの事業継続の方針および実施計画は、ISO 27001に則り定義され、検証されています。 詳細については、ISO 27001の附属書 A.n 14.1 およびSOC1タイプ2レポートで確認する事が出来ます。
		運15	障害時・災害時マニュアルを整備すること。	
	アクセス権限の管理	運16	各種資源、システムへのアクセス権限を明確にすること。	ISO 27001に則り、AWSリソースへの論理的なアクセスのために必要な手順やポリシーを定めています。 SOC1タイプ2レポートには、AWSリソースへのアクセスを管理するためのコントロール方法についての概要が記載されています。
		運17	パスワードが他人に知られないための措置を講じておくこと。	

基準大項目	中項目	項番	小項目	AWS回答
		運18	各種資源、システムへのアクセス権限の付与、見直し手続きを明確化すること。	また詳細については、 AWSのセキュリティ·プロセス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
	オペレーション管理	運19	オペレータの資格確認を行うこと。	AWSは、社員が個々の役割と責任を理解するのを助けるための、内部コミュニケーションのためのさまざまな方策を実施しています。これらの方策は、新入社員研修や、ビジネス成果の確認の面談、またビデオ会議、電子メールやAmazonのイントラネットを介した情報の掲載などの電子的手段も含まれます。 追加情報については、http://aws.amazon.com/securityで入手可能なホワイトペーパーである"セキュリティ·プロセスのAmazon Web Servicesの概要"を参照してください。
		運20	オペレーションの依頼・承認手続きを明確にすること。	
		運21	オペレーション実行体制を明確にすること。	
		運22	オペレーションの記録、確認を行うこと。	
		運23	クライアントサーバー・システムにおける作業の管理を行うこと。	
	入力管理	運24	データの入力管理を行うこと。	AWS利用者は、データのコントロールと所有権を保持しており、データ入力を管理することは利用者の責任となります。
	データファイル管理	運25	授受・管理方法を定めること。	AWS利用者は、データの所有権と、データ転送やデータファイルのリビジョン管理などのコントロールを行なう所有権を保持します。 AWSは、利用者のインスタンスやデータを、複数のアベイラビリティゾーンや複数のリージョンに配置できる柔軟性を提供します。利用者がAWSを利用する場合は、複数のリージョンやアベイラビリティゾーンが利用出来る利点を生かし、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置するなど、自然災害も含めたシステム障害に対して柔軟に対応できるシステム設計を行なうことが出来ます。
		運26	修正管理方法を明確にすること。	
		運27	バックアップを確保すること。	
	プログラムファイル管理	運28	管理方法を明確にすること。	AWS利用者は、データやプログラムファイルのコントロールと所有権を保持しており、それらの管理は利用者の責任となります。
		運29	バックアップを確保すること。	

基準大項目	中項目	項番	小項目	AWS回答
	コンピュータウイルス対策	運30	コンピュータウイルス対策を講ずること。	AWSのプログラム、プロセス、およびアンチウイルス/悪意のあるソフトウェアを管理するための手順は、ISO 27001規格に準拠しています。また SOC1タイプ2のレポートで詳細情報を提供しています。 さらに追加の詳細については、ISO 27001規格のAppendix A.10.4を参照してください。 AWSは独立した監査人によって検証され、ISO 27001認証に準拠することが確認されています。
	ネットワーク設定情報管理	運31	設定情報の管理を行うこと。	AWSインフラストラクチャに対する緊急時や非ルーチン作業を含む構成の変更については全て認可、記録、テスト、承認され、また標準に従い文書化されます。 追加情報については、http://aws.amazon.com/securityで入手可能なホワイトペーパー"AWSのセキュリティ･プロセスの概要"を参照してください。
		運32	設定情報のバックアップを確保すること。	
	ドキュメント管理	運33	保管管理方法を明確にすること。	AWS利用者は、データの所有権と、それらのコントロールやストレージ管理を行なうための処理を行なう事が出来ます。
		運34	バックアップを確保すること。	
	帳票管理	運35	未使用重要帳票の管理方法を明確にすること。	AWS利用者は、データやそれに関連する帳票の所有権を保持しており、それらの管理は利用者の責任となります。
		運36	重要な印字済帳票の取扱方法を明確にすること。	
	出力管理	運37	出力情報の作成、取扱いについて、不正防止および機密保護対策を講ずること。	AWS利用者は、データやそれに関連する出力物の所有権を保持しており、それらの管理は利用者の責任となります。
	取引の管理	運38	各取引の操作権限を明確にすること。	AWS利用者は、データやそれに関連する取引についての所有権を保持しており、それらの管理は利用者の責任となります。
		運39	オペレータカードの管理を行うこと。	
		運40	取引の操作内容を記録・検証すること。	
		運41	顧客からの届出の受付体制を整備し、事故口座の管理を行うこと。	
		運42	機器および媒体の盗難、破損等に伴い、利用者が被る可能性がある損失および責任を明示すること。	

基準大項目	中項目	項番	小項目	AWS回答
	暗号鍵の管理	運43	暗号鍵の利用において運用管理方法を明確にすること。	AWS利用者はAWSが提供するサーバサイド暗号化サービスを利用していない限り、利用者自身で暗号化に関する管理を行なう必要があります。 S3,EBS,SimpleDBやEC2など、ほぼ全てのシステムは利用者により暗号化を行なう事が出来ます。VPCの接続セッションは暗号化されています。Amazon S3はオプションとして、サーバサイドの暗号化サービスを提供しています。AWS利用者は、3rdパーティーの暗号化技術を利用する事が出来ます。 AWSで管理しているキーの管理手順は、ISO 27001規格に準拠しています。 さらに追加の詳細については、ISO 27001 附属書A.15.1を参照してください。 AWSは独立した監査人によって検証され、ISO 27001規格に準拠することが確認されています。
	厳正な本人確認の実施	運44	本人確認を行うこと。	AWS利用者は、金融トランザクションを行なうためのデータやデータの制御を行なう事が出来、それらの管理は利用者の責任となります。
		運44-1	CD・ATM等の機械式預貯金取引における正当な権限者の取引を確保すること。	
	CD・ATM等および無人店舗の管理	運45	運用管理方法を明確にし、かつ不正払戻防止の措置を講ずること。	AWS利用者は、金融トランザクションを行なうためのデータやデータの制御を行なう事が出来、それらの管理は利用者の責任となります。
		運46	監視体制を明確にすること。	
		運47	防犯体制を明確にすること。	
		運48	障害時・災害時の対応方法を明確にすること。	
		運49	関係マニュアルの整備を行うこと。	
	渉外端末の管理	運50	運用管理方法を明確にすること。	AWS利用者は、渉外端末に関するデータやデータの制御を行なう事が出来、それらの管理は利用者の責任となります。
	カード管理	運51	カードの管理方法を明確にすること。	AWS利用者は、カードに関するデータやデータの制御を行なう事が出来、それらの管理は利用者の責任となります。
		運51-1	顧客に対して犯罪に関する注意喚起を行うこと。	
		運52	指定された口座のカード取引監視方法を明確にすること。	
	顧客データ保護	運53	顧客データの保護策を講ずること。	AWS利用者は、顧客や生体認証に関するデータやデータの制御を行なう事が出来、それらの管理は利用者の責任となります。
		運53-1	生体認証における生体認証情報の安全管理措置を講ずること。	
	資源管理	運54	能力および使用状況の確認を行うこと。	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、リソースの能力や使用状況を把握することができ、それらの管理は利用者の責任となります。
	外部接続管理	運55	接続契約内容を明確にすること。	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、外部との接続管理を行なう事が出来ます。またその管理は利用者の責任となります。
		運56	外部接続における運用管理方法を明確にすること。	
	機器の管理	運57	管理方法を明確にすること。	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、利用者の機器に対する管理

基準大項目	中項目	項番	小項目	AWS回答
		運58	ネットワーク関連機器の保護措置を講ずること。	を行なう事ができます。またその管理は利用者の責任となります。
		運59	保守方法を明確にすること。	
	運行監視	運60	監視体制を整備すること。	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の監視機能を提供します。詳細については、aws.amazon.com/cloudwatch を参照して下さい。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。 status.aws.amazon.comを参照して下さい。
	コンピュータ室・データ保管室の管理	運61	入室後の作業を管理すること。	物理的アクセスは、入退室や各境界で厳密に管理されています。アクセスを許可された従業員は、データセンターに入るために2要素認証を最低2回パスする必要があります。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行されます。
	障害時・災害時対応策	運62	関係者への連絡手順を明確にすること。	AWSは、利用者のインスタンスやデータを、複数のアベイラビリティゾーンや複数のリージョンに配置できる柔軟性を提供します。利用者がAWSを利用する場合は、複数のリージョンやアベイラビリティゾーンが利用出来る利点を生かし、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置するなど、自然災害も含めたシステム障害に対して柔軟に対応できるシステム設計を行なうことが出来ます。 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。
		運63	障害時・災害時復旧手順を明確にすること。	
		運64	障害の原因を調査・分析すること。	
	コンティンジェンシープランの策定	運65	コンティンジェンシープランを策定すること。	AWSのビジネス継続のポリシーやプランはISO27001規格に準拠する形で定義・検証されています。 AWSのビジネス継続に関する詳細は、ISO27001規格の附属書 A. 14.1やSOC1レポートを参照して下さい。
システム開発・変更	**ハードウェア・ソフトウェア管理**	運66	ハードウェア、ソフトウェアの管理を行うこと。	ISO27001規格に準じ、AWSのハードウェア資産はAWS独自の在庫管理ツールを使用してAWSの担当者によって管理、監視されています。 追加の詳細については、ISO27001規格の附属書 A. 7.1を参照して下さい。AWSは独立した監査人によって検証され、ISO 27001規格に準拠することが確認されています。 AWSは、ISO27001規格に準じたシステム開発ライフサイクル（SDLC）プロセスの一環として、社内の品質基準を設けています。 追加の詳細については、ISO27001規格の附属書 A. 10.1を参照して下さい。AWSは独立した監査人によって検証され、ISO 27001規格に準拠することが確認されています。

基準大項目	中項目	項番	小項目	AWS回答
	システム開発・変更管理	運67	開発・変更手順を明確にすること。	AWS利用者は、本番環境及びテスト環境を構築する権利と責任を有しています。AWSのWebサイトでは、AWSのサービスを使用して環境を構築するガイダンスを提供しています。http://aws.amazon.com/documentation/
		運68	テスト環境を整備すること。	
		運69	本番への移行手順を明確にすること。	
	ドキュメント管理	運70	作成手順を定めること。	ISO27001規格に準じ、AWSは重要なコンポーネントに対するシステム要件を明文化しています。ISO27001規格の附属書 A. 12.1を参照して下さい。AWSは独立した監査人によって検証され、ISO 27001規格に準拠することが確認されています。
		運71	保管管理方法を明確にすること。	
	パッケージの導入	運72	評価体制を整備すること。	AWS利用者は、ゲストＯＳ,ソフトウェアおよびアプリケーションの制御を行なう事ができ、それらのパッケージの管理は利用者の責任となります。
		運73	運用・管理体制を明確にすること。	
	システムの廃棄	運74	廃棄計画、手順を策定すること。	ISO27001規格に準じ、ストレージデバイスを破棄する場合、AWS利用者のデータが漏洩する事を防ぐための破棄プロセスを定めています。 このプロセスでは、データを破壊する方法としてDoD 5220.22-M (“National Industrial Security Program Operating Manual”) またはNIST 800-88 (“媒体のサニタイズに関するガイドライン”)に準じた方法を使用しています。 もしハードウェアデバイスが上記手順でデータ破壊出来ない場合、業界の標準的な方法で消磁や物理的な破壊を行ないます。
		運75	情報漏洩防止対策を講ずること。	
各種設備管理	**保守管理**	運76	管理方法を明確にすること。	AWSはセキュリティ、生存維持システムおよび機器に対して電気的、機械的、物理的にモニタリングしており、問題が発生した場合は即座に検知します。機器の継続的な利用のために、予防保全作業を行なっています。 追加情報に関しては「Amazon Web Servicesセキュリティプロセス概要」のホワイトペーパーを参照して下さい。http://aws.amazon.com/security
		運77	保守方法を明確にすること。	
	資源管理	運78	能力および使用状況の確認を行うこと。	サービスのアベイラビリティを効果的に管理するため、AWSによりリソース利用率はモニタリングされます。
	監視	運79	監視体制を整備すること。	AWSはセキュリティ、生存維持システムおよび機器に対して電気的、機械的、物理的にモニタリングしており、問題が発生した場合は即座に検知します。 Cloudwatchは、AWSのクラウド資源及び顧客が運用するアプリケーションに対するモニタリングを提供します。詳細についてはhttp://aws.amazon.com/cloudwatchをご参照ください。また、AWSはサービス提供状況における最新の情報をService Health Dashboardにて公開しています。http://status.aws.amazon.comをご参照ください。
教育・訓練		運80	セキュリティ教育を行うこと。	AWSは、社員が個々の役割と責任を理解するのを助けるための、内部コミュニケーションのためのさまざまな方策を実施しています。これらの方策は、新入社員研修や、ビジネス成果の確認の面談、またビデオ会議、
		運81	要員に対するスキルアップ教育を行うこと。	

基準大項目	中項目	項番	小項目	AWS回答
		運82	オペレーション習熟のための教育および訓練を行うこと。	電子メールやAmazonのイントラネットを介した情報の掲載などの電子的手段も含まれます。 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
		運83	障害時・災害時に備えた教育・訓練を行うこと。	
		運84	防災・防犯訓練を行うこと。	
要員管理		運85	要員の人事管理を適切に行うこと。	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
		運86	要員の健康管理を行うこと。	
外部委託管理	**外部委託に関する計画**	運87	システムの開発や運用等で外部委託を行う場合は、事前に目的や範囲を明確にすること。	外部委託先の管理については、AWS利用者の責任となります。
		運87-1	外部委託先の選定手続きを明確にすること。	
		運88	安全対策に関する項目を盛込んだ委託契約を締結すること。	
	外部委託業務管理	運89	外部委託先の要員にルールを遵守させ、その遵守状況を管理、検証すること。	外部委託先の管理については、AWS利用者の責任となります。
		運90	外部委託における業務組織の整備と業務の管理、検証を行うこと。	
		運90-1	金融機関相互のシステム・ネットワークのサービス利用にあたっては、適切なリスク管理を行うこと。	
システム監査	**システム監査(システム監査)**	運91	システム監査体制を整備すること。	AWSは、特定の業界の認定および独立した第三者の証明を取得し、特定の証明書、レポート、およびNDAの下で直接AWS利用者にこれらの関連ドキュメントを提供しています。 AWS利用者は、コントロールとそのデータの所有権を保持しており、従って自身の環境に対する監査手続を策定するのは、利用者の責任となります。
インストアブランチ		運92	出店先の選定基準を明確にすること。	
コンビニATM		運93	出店先の選定基準を明確にすること。	
		運94	現金装填等メンテナンス時の防犯対策を講じること。	
		運95	障害時・災害時対応手順を明確にすること。	
		運96	ネットワーク関連機器、伝送データの安全対策を講ずること。	

基準大項目	中項目	項番	小項目	AWS回答
		運97	所轄の警察および警備会社等関係者との連絡体制を確立すること。	
		運98	顧客に対して犯罪に関する注意喚起を行うこと。	
デビットカード	**デビットカード・サービスの安全性確保**	運99	デビットカード・サービスにおける安全対策を講ずること。	金融サービスのセキュリティやデビッドカードサービスのセキュリティについての管理は、AWS利用者の責任となります。
		運100	口座番号、暗証番号等の安全性を確保すること。	
	顧客保護	運101	デビットカード利用時の顧客保護の措置を講ずること。	顧客に対して提供する金融サービスのセキュリティについての管理は、AWS利用者の責任となります。
	顧客への注意喚起	運102	デビットカード利用上の留意事項を顧客に注意喚起すること。	
オープンネットワークを利用した金融サービス	**インターネット、モバイル**	運103	不正使用を防止すること。	クライアントアプリケーションやモバイルアプリケーションの管理は、AWS利用者自身の要求に基づき管理することが出来ます。
		運104	不正使用を早期発見すること。	
		運105	安全対策に関する情報開示をすること。	
		運105-1	顧客対応方法を明確にすること。	
		運106	インターネットやモバイル等を用いた金融サービスの運用管理方法を明確化すること。	
	電子メール	運107	電子メールの運用方針を明確にすること。	電子メールの運用ポリシーについては、AWS利用者自身の要求に基づき管理することが出来ます。
ハードウェアの信頼性向上対策	**ハードウェアの障害予防策**	技1	予防保守を実施すること。	AWSは、電気的、機械的、物理的セキュリティ及び生命維持に関するシステムと設備を監視し、如何なる問題も速やかに特定されるようにしています。機器の継続的な稼働を維持するため、予防的なメンテナンスも実施します。 追加情報に関しては下記の「Amazon Web Servicesセキュリティプロセス概要」白書をご参照ください。 http://aws.amazon.com/security
	ハードウェアの予備	技2	本体装置の予備を設けること。	AWSは顧客に対して、複数の地域や異なるアベイラビリティゾーンにインスタンスを配置したり、データを保存したりする柔軟性を提供します。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。障害に際しては、自動化されたプロセスにより顧客のデータトラフィックは影響のあるエリアから退避されます。AWS SOC 1タイプ2レポートにさらなる詳細が記載されています。ISO27001 附属書 A,. 11.2に追加情報があります。AWSは独立した監査人によって検証され、ISO 27001認証への準拠が確認されています。
		技3	周辺装置の予備を設けること。	
		技4	通信系装置の予備を設けること。	
		技5	回線の予備を設けること。	
		技6	端末系装置の予備を設けること。	

基準大項目	中項目	項番	小項目	AWS回答
ソフトウェアの信頼性向上対策	**開発時の品質向上対策**	技7	システム開発計画は中長期計画との整合性を確認するとともに、承認を得ること。	AWSは、変更の管理に体系的なアプローチを採用し、顧客に影響を与えるサービスの変更は徹底的な検証・試験・承認及び充分な情報提供がなされるようになっています。 追加情報に関しては下記の「Amazon Web Services セキュリティプロセス概要」白書をご参照ください。 http://aws.amazon.com/security
		技8	必要となるセキュリティ機能を取り込むこと。	
		技9	設計段階でのソフトウェアの品質を確保すること。	
		技10	プログラム作成段階での品質を確保すること。	
		技11	テスト段階でのソフトウェアの品質を確保すること。	
		技12	プログラムの配布を考慮したソフトウェアの信頼性を確保すること。	
		技13	パッケージ導入にあたり、ソフトウェアの品質を確保すること。	
	メンテナンス時の品質向上対策	技14	定型的変更作業時の正確性を確保すること。	AWSは、重要なサービスの変更に対する自己監査により、品質のモニタリング、高い基準の維持、変更管理プロセスの継続的な改善を行っています。
		技15	機能の変更、追加作業時の品質を確保すること。	
運用時の信頼性向上対策		技16	オペレーションの自動化、簡略化を図ること。	AWSの顧客は、運用監視に関する操作を管理する権限と責任を持ち続けます。
		技17	オペレーションのチェック機能を充実すること。	
		技18	負荷状態の監視制御機能を充実すること。	
		技19	CD・ATM等の遠隔制御機能を設けること。	
障害の早期発見・早期回復	**障害の早期発見**	技20	システム運用状況の監視機能を設けること。	AWSでは、電気的、機械的、物理的セキュリティ及び生命維持に関するシステムと設備を監視し、如何なる問題も速やかに特定されるようにしています。顧客は所有するゲストオペレーティングシステム、ソフトウェア、アプリケーションに対する制御権を保持し、また、それらのシステムの状態を論理的にモニタリングする責任を負います。AWS Cloudwatchは、AWSのクラウド資源及び顧客が運用するアプリケーションに対するモニタリングを提供します。詳細についてはhttp://aws.amazon.com/cloudwatchをご参照ください。また、AWSはサービス提供状況における最新の情報をService Health Dashboardにて公開しています。http://status.aws.amazon.comをご参照ください。
		技21	障害の検出および障害箇所の切り分け機能を設けること。	
	障害の早期回復	技22	障害時の縮退・再構成機能を設けること。	AWSの顧客は、自身のデータに対する制御と所有権及び、データファイルの転送管理・リビジョン制御に関する操作を保持します。 AWSは顧客に対し、複数の地域や各リージョン内の異なるアベイラビリティゾーンにインスタンスを配置し
		技23	取引制限機能を設けること。	

基準大項目	中項目	項番	小項目	AWS回答
		技24	リカバリ機能を設けること。	たり、データを保存したりする柔軟性を提供します。複数のアベイラビリティゾーンにアプリケーションを分散配置することで、自然災害やシステム障害を含む多くの障害に対する回復力を保てることから、顧客は複数の地域とアベイラビリティゾーンを活かしたAWSの使用法を設計することが推奨されます。
災害時対策	**バックアップサイト**	技25	バックアップサイトを保有すること。	
データ保護	**漏洩防止**	技26	暗証番号・パスワード等は他人に知られないための対策を講ずること。	AWS環境は、仮想化された、複数テナント環境です。AWSは、セキュリティ管理プロセス、PCI制御及び、各顧客を他の顧客から隔離するセキュリティ制御を実装してきました。AWSシステムは、仮想化ソフトウェアにおいてフィルタすることで、顧客による物理ホスト、割り当てられていないインスタンスへのアクセスを防止するよう設計されています。このアーキテクチャは独立したPCI認定監査機関により検証され、2011年6月に公開されたPCI DSSバージョン2.0における全要求要件を満たすことが確認されました。 詳細については、下記に掲載されたAWSにおけるリスクとコンプライアンス白書をご参照ください。http://aws.amazon.com/security
		技27	相手端末確認機能を設けること。	
		技28	蓄積データの漏洩防止策を講ずること。	
		技29	伝送データの漏洩防止策を講ずること。	
	破壊・改ざん防止	技30	ファイルに対する排他制御機能を設けること。	AWSの顧客は自身のデータに関する制御と所有権を保持し、不良データの検出機能を実装することもできます。
		技31	ファイルに対するアクセス制御機能を設けること。	
		技32	不良データ検出機能を充実すること。	
	検知策	技33	伝送データの改ざん検知策を講ずること。	AWSのデータ管理ポリシーはISO 27001認証に準拠しています。ISO27001 附属書 A. 8.2と11.3をご参照ください。AWSは独立した監査人によって検証され、ISO 27001認証に準拠することが確認されています。AWS SOC 1タイプ2レポートに、AWS上の資源に対する認可されないアクセスを防止するためのAWSにおける取り組みに関する追加の情報が掲載されています。
		技34	ファイル突合機能を設けること。	
不正使用防止	**予防策(アクセス権限確認)**	技35	本人確認機能を設けること。	顧客は所有する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。詳細はAWSのウェブサイトをご参照ください。Http://aws.amazon.com/mfa
		技35-1	生体認証の特性を考慮し、必要な安全対策を検討すること。	
		技36	IDの不正使用防止機能を設けること。	
		技37	アクセス履歴を管理すること。	
	予防策(利用範囲の制限)	技38	取引制限機能を設けること。	AWSの顧客は商取引を制限する権利と責任を保持します。
		技39	事故時の取引禁止機能を設けること。	
	予防策(不正・偽造防止対策)	技40	カードの偽造防止対策のための技術的措置を講ずること。	AWSの顧客はカードの利用を管理・計測する権利と責任を保持します。

基準大項目	中項目	項番	小項目	AWS回答
	物理対策)	技41	電子的価値の保護機能、または不正検知の仕組みを設けること。	
		技42	電子化された暗号鍵を蓄積する機器、媒体、またはそこに含まれるソフトウェアには、暗号鍵の保護機能を設けること。	
		技42-1	電子メール送受信、ホームページ閲覧等の不正使用防止機能を設けること。	
	外部ネットワークからのアクセス制限	技43	外部ネットワークからの不正侵入防止機能を設けること。	AWSは、ISO 27001認証に準拠する中で、AWSの資源への論理的なアクセスに関する最小限の基準を定めるための正式なポリシー及び手順を確立しました。AWS SOC 1タイプ2レポートにおいて、AWS資源へのアクセスプロビジョニングを管理を実現する制御の概要が述べられています。 追加情報に関しては下記の「Amazon Web Servicesセキュリティプロセス概要」白書をご参照ください。 http://aws.amazon.com/security
		技44	外部ネットワークからアクセス可能な接続機器は必要最小限にすること。	
	検知策	技45	不正アクセスの監視機能を設けること。	顧客は所有するゲストオペレーティングシステム、ソフトウェア、アプリケーションに対する制御権を保持し、また、それらのシステムモニタリングする仕組みを開発する責任を負います。 AWSシステムに向け、AWSでは、ISO 27001認証に準拠する中で、AWSの資源への論理的なアクセスに関する最小限の基準を定めるための正式なポリシー及び手順を確立しました。AWS SOC 1タイプ2レポートにおいて、AWS資源へのアクセスプロビジョニングの管理を実現する制御の概要が述べられています。 追加情報に関しては下記の「Amazon Web Servicesセキュリティプロセス概要」白書をご参照ください。http://aws.amazon.com/security
		技46	異常な取引状況を把握するための機能を設けること。	
		技47	異例取引の監視機能を設けること。	
	対応策	技48	不正アクセスの発生に備えて対応策、復旧策を講じておくこと。	顧客は所有するゲストオペレーティングシステム、ソフトウェア、アプリケーションに対する制御権を保持し、また、それらのシステムの状態をモニタリングする仕組みを開発する責任を負います。 AWSのデータ管理ポリシーはISO 27001認証に準拠しています。ISO27001 附属書 A. 8.2と11.3をご参照ください。AWSは独立した監査人によって検証され、ISO 27001認証に準拠することが確認されています。AWS SOC 1タイプ2レポートに、AWS上の資源に対する不正アクセスを防止するためのAWSにおける取り組みに関する追加の情報が掲載されています。

基準大項目	中項目	項番	小項目	AWS回答
不正プログラム防止	**防御策**	技49	コンピュータウイルス等不正プログラムへの防御対策を講ずること。	AWSのプログラム、プロセス群、及びウイルス/マルウェア対策ソフトウェアの管理はISO 27001認証に準拠しています。AWS SOC1 タイプ2レポートにさらなる詳細情報が記載されています。 追加の情報についてはISO27001 附属書 A,. 10.4をご参照ください。AWSは独立した監査人によって検証され、ISO 27001認証への準拠が確認されています。
	検知策	技50	コンピュータウイルス等不正プログラムの検知対策を講ずること。	
	復旧策	技51	コンピュータウイルス等不正プログラムによる被害時対策を講ずること。	

Notices