金融機関向け「Amazon Web Services」対応セキュリティリファレンス
（サマリー版）

FISC 金融情報システムセンター「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
version 1.20

2013/9/11

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

最終更新日 2013/9/11

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

システムインテグレーター等がAWSを利用して、金融機関にシステムを提供する場合のFISCの各安全対策基準（第8版）および（第8版追補）の各項目について、【FISC安全対策基準に対するAWSの見解】、【FISC安全対策基準への適合性】、【クラウド事業者の対応】、【SI事業者・利用者で必要な対応】の分類で整理する。なお、項目によっては、「クラウド事業者」と「SI事業者・利用者」の両方で対応をすべき項目もあり、その両方の結果により【FISC安全対策基準への適合性】が整理される。

【FISC安全対策基準に対するAWSの見解】
FISC安全対策基準の中項目レベルの項目ごとでのAWSの見解を記載。
これらは、Cloud Security Alliance (CSA)のSecurity, Trust & Assurance Registry (STAR)に登録されたアンケート回答からも参照することができる内容と同等である。

【FISC安全対策基準への適合性】
「クラウド事業者の対応状況」ならびに「SI事業者・利用者で必要な対応要否」からFISC安全対策基準の適合性への可能性を整理

FISC安全対策基準への適合性	「適合可能」: FISC安全対策基準への適合は可能 「適合不可」: FISC安全対策基準への適合は不可 「対象外」: クラウド環境における安全対策検討の対象範囲外

【クラウド事業者の対応】 クラウド事業者でのFISC安全対策基準への対応状況

対応状況	「〇」: クラウド事業者で対応実施 「ー」: クラウド事業者では対応の実施不要 「対象外」: クラウド環境における安全対策検討の対象範囲外
開示レベル	「公開情報」: 公開文書に記載されている公開情報 「要NDA」: AWSとのNDA締結により入手できる文書等に記載された情報
実施内容(参照された内容等)	公開文書に記載されている対策実施の内容
公開文書への参照	記載されている公開文書への参照情報
第三者認証から類推出来る内容	第三者認証の認証状況から対応状況が類推できる対応
AWS/ADSJへのインタビュー	AWS/ADSJへのインタビューからの情報
NDAベース資料への参照	AWSとのNDA締結により入手できる文書等への参照情報

【SI事業者・利用者で必要な対応】 SI事業者・利用者でのFISC安全対策基準への対応要否

対応要否	「●」: SI事業者・利用者で対応が必要 「ー」: SI事業者・利用者では対応が不要 「対象外」: クラウド環境における安全対策検討の対象範囲外
対策例	SI事業者・利用者側でのFISC安全対策基準への対応となる対策例

【情報の参照元】

番号	参照元名称/URL
1	AWS セキュリティ&コンプライアンスセンター
	URL　http://aws.amazon.com/jp/security/
2	Amazon Web Services: セキュリティプロセスの概要（2011年5月版：日本語）
	URL　https://d36cz9buwru1tt.cloudfront.net/jp/wp/AWS%20Security%20Whitepaper%20-%20May%202011.pdf
3	Amazon Web Services: リスクとコンプライアンス（2012年7月版：日本語）
	URL　http://d36cz9buwru1tt.cloudfront.net/jp/wp/AWS%20Risk%20and%20Compliance%20Whitepaper%20-%20July%202012%20FINAL.pdf
4	PCI DSS Level 1 Compliance
	URL　http://aws.amazon.com/jp/compliance/pci-dss-level-1-compliance-faqs/
5	PCI-DSSv2.0　ダウンロード先
	URL　https://ja.pcisecuritystandards.org/minisite/en/
6	Amazon Elastic Block Store (EBS)
	URL　http://aws.amazon.com/jp/ebs/
7	Using Regions and Availability Zones
	URL　http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/ ¥ using-regions-availability-zones.html#concepts-regions-availability-zones
8	Amazon Web Services: Overview of Security Processes（June 2013：英語）
	URL　http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf
9	Amazon Web Services: Risk and Compliance（June 2013：英語）
	URL　http://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf

【取得済みの認証と認定】※AWSをご利用されている場合、別途NDAベースにて個別に開示

番号	認証と認定
1	SOC 1(Service Organization Controls 1) Type2 / SSAE 16/ ISAE 3402
2	PCIデータセキュリティ基準のPCI DSS レベル 1
3	情報セキュリティマネジメントシステム（Information Security Management System/ISMS）の ISO 27001
4	SOC 2(Service Organization Controls 2)

【補足事項】
[適用区分]について
※適用区分としては、クラウド環境でのシステム構築／運用に関する「コンピュータセンター」と「ダイレクトチャネル」を選択している。

SI事業者・利用者が対応方法を検討する場合、「FISCガイドラインに記載されている内容で対応可能な場合」と「クラウドの特性を考慮すべき場合」との2つのパターンに分類することができる。さらに、「クラウドの特性を考慮する場合」には、「セキュリティベンダー等が提供する機能で対応できる場合（クラウドでの一般的対応方法）」「クラウド事業者が提供するサービスを活用し対応できる場合（AWS特有の対応方法）」に分類することができる。
これらを「対応パターン」として各項目ごとに分類し、対応すべきあるいは対応が推奨される機能・サービスを明確にした。

【対応パターンの分類】

パターン1	FISCガイドラインに記載されている、従来どおりの内容で対応可能な場合。 （対策例の記載方法）「適用にあたっての考え方」から抜粋または、引用し対応方法を記述している。
パターン2	クラウドの特性を考慮し対応可能であり、かつ、AWSのサービスを使用して対応可能な場合。 （対策例の記載方法）「対策例」の記載に加えて、「AWS特有の対応方法」をサービスごとに明確にしている。
パターン3	クラウドの特性を考慮し対応可能であるが、暗号化・アンチウィルス等の機能を使用して対応可能な場合。 （対策例の記載方法） 本バージョンでは、非公開としている。

【対応方法の考え方】
対応方法には、「機能（製品、ツール含む）」を使用すれば実現可能な場合もあれば、単に機能を使うのではなく、いくつかの手続きをへて実現可能となる「プロセス」によるものもあり、対応方法ではこれらを区分した。
また、それらの方法を利用するにあたり、必ず利用することになるあるいは利用すべきものを「必須」とし〇で、利用することでより効率的あるいは安全性が高まるものを「推奨」として△で記した。

【クラウドでの一般的対応方法】

対応方法	説明
暗号化	利用者はデータをクラウドへアップロードする前に暗号化する。また、クライアント（端末）・インスタンス（仮想サーバ）間等インスタンスとの間でデータを通信する場合に暗号化する。
Antivirus	利用者はインスタンスにセキュリティベンダーが提供するアンチウィルスソフトを導入し、インスタンスおよびデータを保護する。 また、インスタンスを作成する前およびデータをインスタンスへアップロードする前にウィルスへ感染していないことを確認する。
FW/IDS/IPS	利用者はインタンスを保護するために、ホスト型のFW（ファイアウォール）やIDS、IPSを導入する。
キー・署名の外部管理	クラウド管理ツールへアクセスするためのキーやその他署名などは、なりすましなどの不正アクセスの抑制や障害からの回復のために、外部へ暗号化などを行い安全に保管する。
証跡等の保管場所	ログや記録等の証跡は監査への対応や不正アクセス、障害の原因追跡のために、損失や改ざん等ができないように保護し外部へ保管する。

【AWS特有の対応方法】

対応方法	説明
API	「Amazon EC2 API Tools」で提供されるAPIを使用し、利用者はAWSをコントロールしログや証跡を取得できる。
	http://aws.amazon.com/developertools/351
IAM	AWS Identity and Access Management (IAM) により、ユーザーが可能な操作を管理者はコントロールできる。
	http://aws.amazon.com/jp/iam/
VPC	Amazon Virtual Private Cloud（Amazon VPC） では、仮想ネットワークを定義できる。また、サブネットの作成、ルーティングの設定など、仮想ネットワーク環境をコントロールすることができる。
	http://aws.amazon.com/jp/vpc/
Multi-AZ	各々独立したロケーション（AZ：Availability Zone）間をAPIを使用しコントロールすることで、障害に対する回復をより俊敏に行える。
	https://d36cz9buwru1tt.cloudfront.net/jp/wp/AWS%20Security%20Whitepaper%20-%20May%202011.pdf
CloudWatch	Amazon CloudWatch により、AWS リソースのメトリックスや独自のカスタムアプリケーションやシステムメトリックスを監視できる。また、アラームの設定もできる。
	http://aws.amazon.com/jp/cloudwatch/
EBS/ Snapshot	Amazon EBS（Amazon Elastic Block Store） は、ボリュームの特定時点のスナップショットを作成して、S3 に保管することができる。このスナップショットを使用し、緊急時に新しいEBSボリュームを立ち上げることや、データの長期間保管ができる。
	http://aws.amazon.com/jp/ebs/
Auto Scaling	Auto Scaling により、利用者が定義する条件に応じて、Amazon EC2 の能力を、自動的に縮小・拡張することができる。
	http://aws.amazon.com/jp/autoscaling/
ELB	Elastic Load Balancing（ELB）は、複数の Amazon EC2 インスタンス間で、アプリケーショントラフィックの負荷を自動的に分散できる。これを使用し耐障害性に優れたアプリケーション運用を可能にする。
	http://aws.amazon.com/jp/elasticloadbalancing/
Management Console	ウェブベースのユーザーインターフェイスを使用して、アマゾン ウェブ サービスにアクセスして管理できる。
	http://aws.amazon.com/jp/console/
Security Group	ファイヤウォール（セキュリティグループ）を使用して、IPプロトコル、サービスポート、ソース／宛先 IP アドレスでトラフィックを制限することができる。
	https://d36cz9buwru1tt.cloudfront.net/jp/wp/AWS%20Security%20Whitepaper%20-%20May%202011.pdf
Direct Connect	AWS Direct Connect により、利用者の環境からAWSへの専用ネットワーク接続を確立することができる。
	http://aws.amazon.com/jp/directconnect/
AWSサポート	技術サポートエンジニアが24時間365日、年中無休での対応を受けることが可能である。
	http://aws.amazon.com/jp/premiumsupport/

FISC 安全対策基準第8版および第8版追補からの引用									FISC安全対策基準に対するAWSの見解	FISC 安対基準への適合性	クラウド事業者の対応 (Amazon Web Services)							SI事業者・利用者で必要な対応			クラウド特有の対応方法　○・・・対応必須、△・・・対応推奨																			
																						クラウドの一般的対応方法				AWS特有の対応方法																
																						実装				実装														プロセス
SEQ	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	必須とされている項目	第8版追補での改訂	追108関連			対応状況	開示レベル	実施内容 （参照された内容等）	公開文書への参照	第三者認証から類推出来る内容	AWS/ADSJへのインタビュー結果	NDAベース資料への参照	対応要否	対応パターン	対策例	暗号化	Antivirus	FW/IDS/IPS	キー・署名の外部管理	証跡等の保管場所	API	IAM	VPC	Multi-AZ	CloudWatch (EC2)	EBS/Snap Shot(EC2)	Auto Scaling (EC2)	ELB (EC2)	Management Cosole	Security Group	Direct Connect	AWSサポート
A3900001	設1	IV　設備基準 I. コンピュータセンター	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。	コンピュータセンターへの災害の影響を少なくするため、各種災害および障害が発生しやすい地域の立地を避けることが望ましい。	○	■		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ご参照してください。 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、SOC2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。	適合可能	○	公開情報	・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。	・Amazon Web Services: セキュリティプロセスの概要 / 事業継続性管理				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A4100001	設2	IV　設備基準 I. コンピュータセンター	建物(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。	コンピュータセンターへの災害の影響を少なくするため、コンピュータセンターの自然環境、地域環境等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が望ましい。	○			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立っています。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、SOC2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。	適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A4200001	設3	IV　設備基準 I. コンピュータセンター	建物(周囲)	設3 敷地には通路を確保すること。	敷地には火災時の安全かつ適切な消火活動、避難を容易にするため、建築基準法に定められた幅員の通路を確保すること。	○					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A4300001	設4	IV　設備基準 I. コンピュータセンター	建物(周囲)	設4 隣接物との間隔を十分に取ること。	延焼の防止および消火活動を容易にするため、隣接する建物との間隔を十分取ることが望ましい。	○					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A4400001	設5	IV　設備基準 I. コンピュータセンター	建物(周囲)	設5 塀または柵および侵入防止装置を設けること。	敷地内への不法侵入、建物等の破壊行為を防止するため、敷地境界において入退管理を行う場合は原則として塀を設けることが望ましく、必要に応じて侵入防止装置を設けることが望ましい。	○					適合可能	○	公開情報	・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。	・Amazon Web Services: セキュリティプロセスの概要 / 物理的セキュリティ				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A4500001	設6	IV　設備基準 I. コンピュータセンター	建物(周囲)	設6 看板等を外部に出さないこと。	外部からの侵入、破壊行為等の入為的災害を未然に防止するため、コンピュータセンター等の所在を示した表示板、看板等は外部に出さないことが望ましい。	○					適合可能	○	公開情報	・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。	・Amazon Web Services: セキュリティプロセスの概要 / 物理的セキュリティ				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A4600001	設7	IV　設備基準 I. コンピュータセンター	建物(周囲)	設7 建物には避雷設備を設置すること。	落雷による障害、事故を防止するため、周囲に高い建物がない場合または落雷多発地域においては、建物には避雷設備を設置することが望ましい。	○					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A4700001	設8	IV　設備基準 I. コンピュータセンター	建物(周囲)	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。	安全管理の徹底のため、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が望ましい。	○					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A4800001	設9	IV　設備基準 I. コンピュータセンター	建物(周囲)	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。	コンピュータシステムのサービス中断を防止するため、敷地内の通信回線・電力線は、工事中外部からの侵入等による切断・延焼の防止措置を講ずることが望ましい。	○					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A5000001	設10	IV　設備基準 I. コンピュータセンター	建物(構造)	設10 耐火建築物であること。	防火対策のため、コンピュータセンターの建物は、建築基準法に規定する耐火建築物とすること。	◎			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。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、SOC2タイプ2レポートを参照してください。	適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A5100001	設11	IV　設備基準 I. コンピュータセンター	建物(構造)	設11 構造の安全性を有すること。	コンピュータシステムに障害を及ぼさないため、建築基準法に規定する構造の安全性を有すること。	◎					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A5200001	設12	IV　設備基準 I. コンピュータセンター	建物(構造)	設12 外壁、屋根等は十分な防水性能を有すること。	コンピュータシステムに障害を及ぼさないため、外壁、屋根等は漏水の防止措置を講ずること。	◎					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A5300001	設13	IV　設備基準 I. コンピュータセンター	建物(構造)	設13 外壁等に強度を持たせること。	コンピュータ関連設備を破壊行為等から防御するため、公道等外部に面する外壁等は、強度を持たせることが望ましい。	○					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A5500001	設14	IV　設備基準 I. コンピュータセンター	建物(開口部)	設14 窓には防火措置を講ずること。	延焼を防止するため、延焼のおそれのある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。 AWS SOC1タイプ2、SOC2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。	適合可能	○	公開情報	・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。	・Amazon Web Services: セキュリティプロセスの概要 / 環境的なセーフガード / 火災検出と鎮火				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A5600001	設15	IV　設備基準 I. コンピュータセンター	建物(開口部)	設15 防犯措置を講ずること。	コンピュータセンター建物内への不法な侵入等を防止するため、外部から容易に接近、侵入できる1階等の窓には、防犯措置を講ずること。	◎					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A5700001	設16	IV　設備基準 I. コンピュータセンター	建物(開口部)	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。	入退館管理を確実に行うことによる不法侵入の防止、不審物品の搬出入防止のため、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が望ましい。	○					適合可能	○	公開情報	・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。	・Amazon Web Services: セキュリティプロセスの概要 / 物理的セキュリティ				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A5800001	設17	IV　設備基準 I. コンピュータセンター	建物(開口部)	設17 非常口を設けること。	災害時の安全な避難と非常時持出しの円滑化のため、適切な位置に非常口を設けること。	◎					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A5900001	設18	IV　設備基準 I. コンピュータセンター	建物(開口部)	設18 防水措置を講ずること。	浸水および漏水によるコンピュータ機器等への障害を防止するため、出入口、窓、機器の搬出入口等の開口部は、防水措置を講ずることが望ましい。	○					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A6000001	設19	IV　設備基準 I. コンピュータセンター	建物(開口部)	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。	防犯・防災のため、出入口には十分な強度を有する扉を設置し、錠を付けること。	◎					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A6200001	設20	IV　設備基準 I. コンピュータセンター	建物(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。	要員およびコンピュータシステムを守るため、内装等には、建築基準法に規定する不燃材料および消防法に規定する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、SOC2タイプ2レポートを参照してください。	適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A6300001	設21	IV　設備基準 I. コンピュータセンター	建物(内装等)	設21 地面による内装等の落下・損壊の防止措置を講ずること。	要員およびコンピュータシステムに被害を及ぼさないようにするため、地面による内装等の落下・損壊の防止措置を講ずることが望ましい。	○					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A6600001	設22	IV　設備基準 I. コンピュータセンター	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。	コンピュータシステムへの影響を防止するため、地震、火災、浸水等の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、SOC2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。	適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A6700001	設23	IV　設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(位置)	設23 外部から容易に入れない位置に設置すること。	侵入、破壊、機密漏洩等を防止するため、出入口付近およびエレベータまたは階段で直接入れる位置を避けて設置すること。	◎					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A6800001	設24	IV　設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(位置)	設24 室名等の表示は付さないこと。	侵入、破壊、機密漏洩等を防止するため、コンピュータ室・データ保管室の室名等の表示は付さないこと。	◎					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A6900001	設25	IV　設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(位置)	設25 必要室間を確保すること。	保守、避難のため、必要室間を確保すること。	◎					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A7000001	設26	IV　設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(位置)	設26 専用の独立した室とすること。	安全管理の徹底のため、専用の独立した室とすること。	◎					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A7200001	設27	IV　設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(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。	入退室管理を確実に行うため、常時利用する出入口は1カ所とすることが望ましい。また、安全性を保ち、外部からの熱、湿気、塵埃の侵入を防止するため、常時利用する出入口には、前室を設けることが望ましい。	○			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、手段はこの限りではない）。 AWS SOC1タイプ2、SOC2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。	適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A7300001	設28	IV　設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(開口部)	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。	防犯・防災のため、出入口には十分な強度を有する扉を設置し、錠を付けること。	◎					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A7400001	設29	IV　設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(開口部)	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。	防犯・防災のため、窓を設ける場合は防火・防水措置および窓ガラスの破損防止措置を講じ、さらに外部から室内の機器等が見えない措置を講ずること。	◎					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A7500001	設30	IV　設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(開口部)	設30 非常口、避難器具、誘導灯等を設置すること。	災害時の避難と非常時出しの円滑化のため、コンピュータ室には適切な位置に非常口および避難器具を設置すること。また、非常口への誘導灯および誘導標識を設置すること。	◎					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A7700001	設31	IV　設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(構造・内装等)	設31 独立した防火区画とすること。	建物内他区画からの火災の延焼防止のため、コンピュータ室・データ保管室は、建築基準法に規定する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、SOC2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。	適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A7800001	設32	IV　設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(構造・内装等)	設32 漏水防止対策を講ずること。	建物、設備等の損傷およびコンピュータ機器等に対する障害を未然に防止するため、天井、壁、床面からの漏水防止対策を講ずること。	◎					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A7900001	設33	IV　設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(構造・内装等)	設33 静電気の防止措置を講ずること。	コンピュータシステムへの悪影響を防止するため、コンピュータ室の床表面材料は、静電気の発生、帯電等による影響を防止する措置を講ずること。	◎					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A8000001	設34	IV　設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(構造・内装等)	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。	要員およびコンピュータシステムを火災による被害から守るため、内装等には、建築基準法に規定する不燃材料および消防法に規定する防炎性能を有するものを使用すること。	◎					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A8100001	設35	IV　設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(構造・内装等)	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。	要員およびコンピュータシステムへ被害を及ぼさないようにするため、開仕切壁、天井、照明器具等、地震の際に落下・損壊の危険のあるものは、落下・損壊防止措置を講ずること。	◎					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A8200001	設36	IV　設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(構造・内装等)	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。	地震時に損壊することのないよう、フリーアクセス床は耐震措置を講ずること。	◎					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A8400001	設37	IV　設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(設備)	設37 自動火災報知設備を設置すること。	火災が発生した場合、早期に発見、通報して、初期消火や避難等ができるように、適切な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、火気の検知と防制、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、SOC2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。	適合可能	○	公開情報	・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。	・Amazon Web Services: セキュリティプロセスの概要 / 環境的なセーフガード / 火災検出と鎮火				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A8500001	設38	IV　設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(設備)	設38 非常時の連絡装置を設置すること。	火災等の異常事態の発生を知らせ、初期消火、避難等について適切な指示を与えるため、非常時の連絡装置を設置すること。	◎					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A8600001	設39	IV　設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(設備)	設39 消火設備を設置すること。	火災時に備えて、適切な消火設備を設置すること。	◎					適合可能	○	公開情報	・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。	・Amazon Web Services: セキュリティプロセスの概要 / 環境的なセーフガード / 火災検出と鎮火				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A8700001	設40	IV　設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(設備)	設40 ケーブルの難燃化、延焼防止措置を講ずること。	ケーブルの燃焼・延焼を防止するため、ケーブルの難燃化措置を講ずることが望ましい。また、防火壁、床等のケーブル貫通部分は延焼防止措置を講ずること。	◎					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A8800001	設41	IV　設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(設備)	設41 排煙設備を設置すること。	火災時に備えて、必要な排煙設備を設置すること。	◎					適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

FISC 安全対策基準第8版および第8版追補からの引用									FISC安全対策基準に対するAWSの見解	FISC 安対基準への適合性	クラウド事業者の対応 (Amazon Web Services)								SI事業者・利用者で必要な対応			クラウド特有の対応方法 ○・・・対応必須、△・・・対応推奨																			
																						クラウドの一般的対応方法					AWS特有の対応方法																
																						実装			プロセス		実装														プロセス	
SEQ	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	必須とされている項目	第8版追補での改訂	追108関連			対応状況	開示レベル	実施内容（参照された内容等）	公開文章への参照	第三者認証から照准出来る内容	AWS/ADSJへのインタビュー結果	NDAベース資料への参照	対応要否	対応パターン	対策例	暗号化	Antivirus	FW/IDS/IPS	キー・署名の外部管理	証跡等の保管場所	API	IAM	VPC	Multi-AZ	CloudWatch (EC2)	EBS/Snap Shot(EC2)	Auto Scaling (EC2)	ELB (EC2)	Management Cosole	Security Group	Direct Connect	AWSサポート
A8900001	設42	IV 設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(設備)	設42 非常用照明設備、携帯用照明器具を設置すること。	火災等の異常事態を当に室内要員が安全に避難できるように、コンピュータ室には、非常用照明設備および携帯用照明器具を設置すること。	◎				適合可能	○	詳細版に記載	–	–	PCI-DSSの要件により、該当設備はあるものの類推される		–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A9000001	設43	IV 設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(設備)	設43 水使用設備を設置しないこと。	漏水によるコンピュータシステムへの影響を防止するため、コンピュータ室・データ保管室に水使用設備を設置しないこと。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A9100001	設44	IV 設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(設備)	設44 地震感知器を設置すること。	コンピュータシステムの運転継続を判断し、データ破壊や電気火災等のニ次災害発生を防止するため、コンピュータ室には地震感知器を設置することが望ましい。	○				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A9200001	設45	IV 設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(設備)	設45 出入口には出入管理設備、防犯設備を設置すること。	不法侵入を防止するため、コンピュータ室・データ保管室の出入口には入退室者を識別、記録する出入管理設備を設置すること。さらに、防犯設備を設置することが望ましい。	○				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A9300001	設46	IV 設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(設備)	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。	コンピュータシステムの予防保全、障害時の原因分析のため、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。	◎				適合可能	○	公開情報	・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。	・Amazon Web Services: セキュリティプロセスの概要／環境的セーフガード／天候と温度				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A9400001	設47	IV 設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(設備)	設47 ネズミの害を防止する措置を講ずること。	ネズミによってケーブルが害を受けることを防止するため、適切な措置を講ずることが望ましい。	○				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A9600001	設48	IV 設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(コンピュータ機器、什器・備品)	設48 什器・備品は不燃性とすること。	引火と火災拡大を防止するため、什器・備品はスチール製品等の不燃性とすること。	◎			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。 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	適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A9700001	設49	IV 設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(コンピュータ機器、什器・備品)	設49 静電気防止措置を講ずること。	コンピュータシステムへの悪影響を防止するため、コンピュータ機器、什器・備品は、静電気防止措置を講ずること。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A9800001	設50	IV 設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(コンピュータ機器、什器・備品)	設50 耐震措置を講ずること。	地震の際に装具やコンピュータ機器に影響を与えないよう、コンピュータ機器および什器等の耐震措置を講ずること。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A9900001	設51	IV 設備基準 I. コンピュータセンター	コンピュータ室・データ保管室(コンピュータ機器、什器・備品)	設51 運搬車等に固定装置を取り付けること。	地震の際に装具やコンピュータ機器に被害を与えないよう、磁気テープ、磁気ディスク等の運搬車等は、制動または固定する装置を取り付けること。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A10100001	設52	IV 設備基準 I. コンピュータセンター	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。	コンピュータシステムへの影響を防止するため、地震、火災、浸水等の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、SOC2タイプ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。	適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A10200001	設53	IV 設備基準 I. コンピュータセンター	電源室・空調機械室	設53 保守点検に必要な空間を確保すること。	機器、装置等の保守点検および災害時の避難のため、必要な広さ、高さの空間を確保すること。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A10300001	設54	IV 設備基準 I. コンピュータセンター	電源室・空調機械室	設54 専用の独立した室とすること。	保守管理および障害の拡大防止のため、他の室とは独立した専用の室とすることが望ましい。	○				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A10400001	設55	IV 設備基準 I. コンピュータセンター	電源室・空調機械室	設55 無窓とし、錠を付けた扉を設置すること。	外部からの侵入防止、防火、防水のため、無窓とすることが望ましく、錠を付けた扉を設置すること。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A10500001	設56	IV 設備基準 I. コンピュータセンター	電源室・空調機械室	設56 耐火構造とすること。	火災による延焼防止のため、耐火構造とすること。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A10600001	設57	IV 設備基準 I. コンピュータセンター	電源室・空調機械室	設57 自動火災報知設備を設置すること。	早期に火災を発見するため、自動火災報知設備を設置すること。	◎				適合可能	○	公開情報	・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。	・Amazon Web Services: セキュリティプロセスの概要／環境的セーフガード／火災検出と鎮火				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A10700001	設58	IV 設備基準 I. コンピュータセンター	電源室・空調機械室	設58 ガス系消火設備を設置すること。	火災時に備えて、全域放出型のガス系消火設備を設置することが望ましい。	○				適合可能	○	公開情報	・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。	・Amazon Web Services: セキュリティプロセスの概要／環境的セーフガード／火災検出と鎮火				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A10800001	設59	IV 設備基準 I. コンピュータセンター	電源室・空調機械室	設59 空調設備の漏水防止措置を講ずること。	漏水による障害を回避するため、冷却水の水漏れ、結露等による漏水の防止措置を講ずること。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A10900001	設60	IV 設備基準 I. コンピュータセンター	電源室・空調機械室	設60 ケーブル、ダクトからの延焼防止措置を講ずること。	延焼を防止するため、ケーブル、ダクトからの延焼防止措置を講ずること。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A11100001	設61	IV 設備基準 I. コンピュータセンター	電源設備	設61 電源設備の容量には余裕を持たせること。	コンピュータシステムに必要な電力を安定的に供給するため、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備えて、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、SOC2タイプ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。	適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A11200001	設62	IV 設備基準 I. コンピュータセンター	電源設備	設62 電源は複数回線で引き込むこと。	受電設備の障害時に備え、電源は複数回線で引き込むこと。	○				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A11300001	設63	IV 設備基準 I. コンピュータセンター	電源設備	設63 良質な電力を供給する設備を設置すること。	コンピュータシステムを安定稼動させるため、良質な電力を供給する設備を設置すること。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A11400001	設64	IV 設備基準 I. コンピュータセンター	電源設備	設64 自家発電設備、蓄電池設備を設置すること。	停電時でもコンピュータシステムを継続して稼働させるため、自家発電設備および蓄電池設備を設置すること。	◎	■			適合可能	○	公開情報	・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。	・Amazon Web Services: セキュリティプロセスの概要／環境的セーフガード／電力				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A11500001	設65	IV 設備基準 I. コンピュータセンター	電源設備	設65 電源設備には避雷設備を設置すること。	落雷による被害を防止するため、電源設備には避雷設備を設置すること。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A11600001	設66	IV 設備基準 I. コンピュータセンター	電源設備	設66 電源設備には耐震措置を講ずること。	地震による移動、損傷等を防止するため、電源設備には耐震措置を講ずること。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A11700001	設67	IV 設備基準 I. コンピュータセンター	電源設備	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。	コンピュータシステムへの影響を最小限にするため、コンピュータ機器への電源の引込みは専用分電盤から専用回路にて配線すること。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A11800001	設68	IV 設備基準 I. コンピュータセンター	電源設備	設68 負荷変動の激しい機器との共用を避けること。	コンピュータシステムに安定して電力を供給するため、コンピュータシステムと負荷変動の激しい機器との電源系統は分けること。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A11900001	設69	IV 設備基準 I. コンピュータセンター	電源設備	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。	電源設備や電気機器等からの影響を防止するため、コンピュータシステムのアースは適切に施工すること。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A12000001	設70	IV 設備基準 I. コンピュータセンター	電源設備	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。	各機器に障害を及ぼさないように、過電流や漏電への措置を講ずること。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A12100001	設71	IV 設備基準 I. コンピュータセンター	電源設備	設71 防災、防犯設備用の予備電源を設置すること。	停電した場合でも防災、防犯設備が作動するように、予備電源を設置すること。	◎	■			適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A12300001	設72	IV 設備基準 I. コンピュータセンター	空調設備	設72 空調設備の能力には余裕を持たせること。	コンピュータ室の温湿度を適切に調整するため、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。 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。	適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A12400001	設73	IV 設備基準 I. コンピュータセンター	空調設備	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。	コンピュータシステムの継続した運用を確保するため、空調設備には安定的に空気調和ができる措置を講ずること。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A12500001	設74	IV 設備基準 I. コンピュータセンター	空調設備	設74 空調設備はコンピュータ室専用とすること。	コンピュータ室の温湿度制御を的確に行うため、空調設備は他の室との共用を避けコンピュータ室専用とすること。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A12600001	設75	IV 設備基準 I. コンピュータセンター	空調設備	設75 空調設備の予備を設置すること。	障害の発生に備えて、主要な空調設備機器については予備を設置することが望ましい。	○				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A12700001	設76	IV 設備基準 I. コンピュータセンター	空調設備	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。	空調設備を安定的に稼動させるため、各種の自動制御装置のほか、機器の異常を迅速に検知する異常警報装置を設置すること。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A12800001	設77	IV 設備基準 I. コンピュータセンター	空調設備	設77 空調設備には侵入、破壊防止対策を講ずること。	コンピュータシステムの運用に支障を来さないようにするため、空調設備には侵入、破壊に対する防止対策を講ずること。	◎				適合可能	○	公開情報	・ビデオ監視カメラや侵入検知システムの設置、専門のセキュリティ・スタッフが建物の入口とその周辺の物理的なアクセス管理を実施している。	・Amazon Web Services: セキュリティプロセスの概要／物理的セキュリティ				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A12900001	設78	IV 設備基準 I. コンピュータセンター	空調設備	設78 空調設備には耐震措置を講ずること。	地震による移動、損傷等を防止するため、空調設備には耐震措置を講ずること。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A13000001	設79	IV 設備基準 I. コンピュータセンター	空調設備	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。	火災時の空調設備の損傷を防止するため、空調設備のダクト等の断熱材料および給排気口は不燃材料とすること。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A13200001	設80	IV 設備基準 I. コンピュータセンター	監視制御設備	設80 監視制御設備を設置すること。	障害発生等を早期に発見するため、電源設備、空調設備、防災設備、防犯設備等の監視制御設備を設置すること。 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	◎			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防備を監視し、如何なる問題も速やかに特定されるようにしています。	適合可能	○	公開情報	・火災検出と鎮火、電力、天候と温度、管理	・Amazon Web Services: セキュリティプロセスの概要／環境的セーフガード				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A13300001	設81	IV 設備基準 I. コンピュータセンター	監視制御設備	設81 中央管理室を設置すること。	電源設備、空調設備、防災設備、防犯設備等の運営管理を円滑にし、かつ有効活用を図るため、これらの設備を集中管理する中央管理室を設置することが望ましい。	○				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A13500001	設82	IV 設備基準 I. コンピュータセンター	回線関連設備	設82 回線関連設備には錠をつけること。	不正アクセス、破壊等の不法行為を防止するため、コンピュータ室外に設置される回線関連設備の機器収容架等には錠を付けること。	◎			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、SOC2タイプレポートに、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。	適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A13600001	設83	IV 設備基準 I. コンピュータセンター	回線関連設備	設83 回線関連設備の設置場所の表示は付さないこと。	部外者に回線関連設備の設置場所を知らせないため、設置場所の表示は付さないこと。	◎				適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A13700001	設83-1	IV 設備基準 I. コンピュータセンター	回線関連設備	設83-1 回線は、専用の配線スペースに設けること。	回線を障害および犯罪から防護し、また、他の電源やケーブル等からのノイズの侵入を防止するため、専用の配線スペースに設けることが望ましい。	○			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。	適合可能	○	詳細版に記載	–	–				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
–	設84～設137は、「本部、営業店等」、「流通・小売店舗との提携チャネル」の基準のため、対象外						■											–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A21500001	運1	V. 運用基準	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。	セキュリティ管理を適切に行うため、セキュリティ管理の具体的手順、責任等を明確にし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。エグゼクティブレベル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よう主導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	適合可能	○	公開情報	・ISO 27001の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要／コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス／AWS の認定とサードパーティによる証明				●	1	システム運用におけるセキュリティ管理範囲を明確にし、管理対象となる仮想マシン（ゲストOS）及びその上で稼働するソフトウェア（ミドルウェアやアプリケーション）、データについて管理方針と手順を整備する。システム運用におけるセキュリティの管理方針と手順の整備を進めるとて、全社的な方針に重大な影響を与えるものがある場合については、経営層の指示、承認を得たとで実施する。	ISO 27001管理策「情報セキュリティのための組織」、「通信及び運用管理／運用の手順及び責任」に従った対策の実施。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A21600001	運2	V. 運用基準	管理体制の確立(セキュリティ管理と責任の明確化)	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。	セキュリティ管理の方法を最適なものとするため、作成された文書については、業務の実態にあっているかを定期的に評価し、必要に応じて改訂すること。	◎				適合可能	○	公開情報	・ISO 27001の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要／コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス／AWS の認定とサードパーティによる証明				●	1	セキュリティ管理方針と手順について、運用業務の実態に合っているか定期的な見直しを行う。	ISO 27001管理策「情報セキュリティのための組織」、「通信及び運用管理／運用の手順及び責任」に従った対策の実施。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

FISC 安全対策基準第8版および第8版追補からの引用									FISC安全対策基準に対するAWSの見解	FISC 安対基準への適合性	クラウド事業者の対応 (Amazon Web Services)							SI事業者・利用者で必要な対応			クラウド特有の対応方法 ○・・・対応必須、△・・・対応推奨																			
																						クラウドの一般的対応方法				AWS特有の対応方法														
																						実装				実装												プロセス
SEQ	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	必須とされている項目	第8版追補での改訂	追108関連			対応状況	開示レベル	実施内容（参照された内容等）	公開文書への参照	第三者認証から醸成出来る内容	AWS/ADSJへのインタビュー結果	NDAベース資料への参照	対応要否	対応パターン	対策例	暗号化	Antivirus	FW/IDS/IPS	キー・署名の外部管理	証跡等の保管場所	API	IAM	VPC	Multi-AZ	CloudWatch (EC2)	EBS/Snap Shot(EC2)	Auto Scaling (EC2)	ELB (EC2)	Management Cosole	Security Group	Direct Connect	AWSサポート
A21700001	運3	V. 運用基準	管理体制の確立(セキュリティ管理と責任の明確化)	運3 セキュリティ管理体制を整備すること。	セキュリティ管理を適切に行うため、セキュリティ管理の責任者等を定め、その職務範囲と権限および責任について定めること。	◎	■	□		適合可能	○	公開情報	・ISO 27001の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001管理策「情報セキュリティのための組織」「通信及び運用管理／運用の手順及び責任」に従った対策の実施。			●	1	セキュリティ管理方針と手順に従ってシステムが運用されていることを管理するためのセキュリティ管理体制（組織、職務範囲、権限等）を整備する。システム運用におけるセキュリティの管理方針と手順の改善を進めるとて、全社的な体制に重大な影響を与えるものがある場合については、経営層の指示、承認を得た上で実施する。	-	-	-	-	-	-	-	-	-	-	-	-	-
A21800001	運4	V. 運用基準	管理体制の確立(セキュリティ管理と責任の明確化)	運4 システム管理体制を整備すること。	システムの安全かつ円滑な運用と不正防止のため、システムの管理手順を定め、管理体制を整備すること。	◎	■	□		適合可能	○	公開情報	・ISO 27001の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001管理策「情報セキュリティのための組織」「通信及び運用管理／運用の手順及び責任」に従った対策の実施。			●	1	管理対象となる仮想マシン（ゲストOS）及びそのとで稼働するソフトウエアについて、システム管理手順を定め、それらの手順を実現する管理体制を整備する。	-	-	-	-	-	-	-	-	-	-	-	-	-
A21900001	運5	V. 運用基準	管理体制の確立(セキュリティ管理と責任の明確化)	運5 データ管理体制を整備すること。	データの安全かつ円滑な運用と不正防止のため、データ管理手順を定め、管理体制を整備すること。	◎		□		適合可能	○	公開情報	・ISO 27001の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001管理策「情報セキュリティのための組織」「通信及び運用管理／運用の手順及び責任」に従った対策の実施。			●	1	管理対象となるデータを明確にした上で、そのデータ管理手順を定め、管理体制を整備する。	-	-	-	-	-	-	-	-	-	-	-	-	-
A22000001	運6	V. 運用基準	管理体制の確立(セキュリティ管理と責任の明確化)	運6 ネットワーク管理体制を整備すること。	コンピュータネットワークの適切かつ効率的な運用と不正アクセス等の防止のため、ネットワークの管理手順を定め、管理体制を整備すること。	◎		□		適合可能	○	公開情報	・ISO 27001の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001管理策「情報セキュリティのための組織」「通信及び運用管理／運用の手順及び責任」に従った対策の実施。			●	1	システム運用環境からAWS環境に接続する箇所を含め、自社システム側のネットワークの管理手順および利用者端末等を管理手順として定め、関係者に周知徹底させることにより、ネットワークの適切かつ効率的で安全な運用を行う。	-	-	-	-	-	-	-	-	-	-	-	-	-
A22200001	運7	V. 運用基準	管理体制の確立(組織の整備)	運7 防災組織を整備すること。	災害の予防および被害軽減のため、防災組織を整備し、責任者を明確にすること。	◎			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、	適合可能	○	詳細版に記載	—	—	SOC1 Control Objective5: Physical Security and Environmental Protection.基準に従った対策の実施。			●	1	システム運用環境における防災対応（責任者の明確化等）を行う。	-	-	-	-	-	-	-	-	-	-	-	-	-
A22300001	運8	V. 運用基準	管理体制の確立(組織の整備)	運8 防犯組織を整備すること。	犯罪を防止するため、防犯組織を整備し、責任者を明確にすること。	◎			ISO27002のヘルスプラクティスおよびPCI 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。	適合可能	○	詳細版に記載	—	—	SOC1 Control Objective5: Physical Security and Environmental Protection.基準に従った対策の実施。			●	1	システム運用環境における防犯対応（責任者の明確化等）を行う。	-	-	-	-	-	-	-	-	-	-	-	-	-
A22400001	運9	V. 運用基準	管理体制の確立(組織の整備)	運9 業務組織を整備すること。	コンピュータシステムに係わる業務を円滑かつ適正に運営するとともに、不正を防止するため、業務範囲および責任と権限を明確にし、相互牽制体制を整備すること。	◎				適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type II、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	・SOC1 Control Objective5: Physical Security and Environmental Protectionおよび Change Management 基準に従った対策の実施。 ・SAS70基準に従った対策の実施。 ・ISO 27001 管理策「通信及び運用管理／職務の分割」に従った対策の実施。			●	1	不正防止策として、開発担当者と運用担当者を分離する。	-	-	-	-	-	-	-	-	-	-	-	-	-
A22600001	運10	V. 運用基準	管理体制の確立(各種規定の整備)	運10 各種規定を整備すること。	コンピュータシステムを円滑かつ適正に運用、管理するため、防災、防犯、業務の各組織における責任と権限を明確にした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。	適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type II、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001管理策「情報セキュリティのための組織／内部組織」に従った対策の実施。			●	1	防災・防犯および業務面における責任者を明確にし、システム運用に必要な規定類を整備する。	-	-	-	-	-	-	-	-	-	-	-	-	-
A22800001	運10-1	V. 運用基準	管理体制の確立(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。	セキュリティ関連文書に定められた事項の遵守状況を確認し、全役職員(外部委員を含む)のセキュリティポリシー・ルールに対する意識やセキュリティレベルの向上を図ること。	◎			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。	適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type II、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001管理策「順守／セキュリティ方針及び標準の順守、並びに技術的順守に従った対策の実施。			●	1	システム運用におけるセキュリティ管理方針と手順の遵守状況を定期的に確認する。	-	-	-	-	-	-	-	-	-	-	-	-	-
A23100001	運11	V. 運用基準	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。	コンピュータセンターへの入館者、およびコンピュータ室、データ保管室等重要な室への入室者を特定するため、資格付与と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1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を参照してください。 http://aws.amazon.com/security さらに、SOC1タイプ2、SOC2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。	適合可能	○	公開情報	・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。	・Amazon Web Services: セキュリティプロセスの概要/物理的セキュリティ	SSAE16/ISAE3402の基準に従った対策の実施。		—	—	—	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A23200001	運12	V. 運用基準	入退管理(入退館(室)管理)	運12 入退館管理を行うこと。	不法侵入、危険物持込み、不法持出し等を防止するため、入退館者の資格確認により、コンピュータセンターの入退館管理を行うこと。	◎				適合可能	○	公開情報	・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。	・Amazon Web Services: セキュリティプロセスの概要/物理的セキュリティ	SSAE16/ISAE3402の基準に従った対策の実施。		—	—	—	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A23300001	運13	V. 運用基準	入退管理(入退館(室)管理)	運13 入退室管理を行うこと。	不法侵入、危険物持込み、不法持出し等を防止するため、コンピュータ室およびデータ保管室等重要な室については、資格確認により入退室管理を行うこと。	◎				適合可能	○	公開情報	・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。	・Amazon Web Services: セキュリティプロセスの概要/物理的セキュリティ	SSAE16/ISAE3402の基準に従った対策の実施。		—	—	—	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A23600001	運14	V. 運用基準	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。	コンピュータシステムを正確かつ安全に運用するとともに、本部・営業店等設置の端末機操作の説得性を予め、事務処理を円滑に行うため、通常時における各種手順(含む操作手順)を定めた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て、AWSの担当者が利用できる環境の説得性を予め、事務処理を円滑に行うため、通常時における各種手順(含む操作手順)を定めたマニュアルを整備すること。 http://aws.amazon.com/security/ご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の組織を参照してください。	適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type II、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	・SOC1 Control Objective6: Incident Handlingの基準に従った対策の実施。 ・ISO 27001管理策「情報セキュリティインシデントの管理」に従った対策の実施。			●	1	通常時における各種手順を定めたシステム運用マニュアルを整備する。そのマニュアルにシステム変更等が発生した場合には、都度見直しを行う。	-	-	-	-	-	-	-	-	-	-	-	-	-
A23700001	運15	V. 運用基準	運用管理(マニュアルの整備)	運15 障害時・災害時マニュアルを整備すること。	障害・災害によるコンピュータシステムへの影響の極小化と早期復旧ならびに本部・営業店等における業務継続のため、障害時・災害時における代替措置、復旧手順および対応方法等について定めたマニュアルを整備するこ。	◎	■	□	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.in 14.1 およびSOC1タイプ2、SOC2タイプ2レポートで確認する事が出来ます。	適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type II、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	・SOC1 Control Objective6 Incident Handlingの基準に従った対策の実施。 ・ISO 27001管理策「情報セキュリティインシデントの管理」に従った対策の実施。			●	1	障害時・災害時における代替措置、復旧手順および対応方法等について定めたマニュアルを整備する。そのマニュアルは定期的に見直しを行う。	-	-	-	-	-	-	-	-	-	-	-	-	-
A23900001	運16	V. 運用基準	運用管理(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。	無資格者によるアクセスを防止するため、コンピュータシステムおよび業務上重要なファイルは、アクセス権限所有者を特定すること。	◎			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、SOC2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。 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	適合可能	○	公開情報	・サービス利用者に発行したAWSアカウント管理のためにアクセス権限管理を実施。 ・ISO 27001を始め、SOC1 Type II、SOC2 Type II、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略、従業員のライフサイクル、Amazon アカウントセキュリティ機能 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	・PCI-DSS、SSAE16/ISAE3402の基準に従った対策の実施。 ・ISO 27001 管理策「資産の管理」「アクセス制御」に従った対策の実施。			●	1	システムとシステムの運用上重要なファイルは、アクセス権限所有者を特定する。	-	-	-	-	-	-	-	-	-	-	-	-	-
A24000001	運17	V. 運用基準	運用管理(アクセス権限の管理)	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。	パスワード等の漏洩防止のため、他人に知られないための注意喚起等の措置を講じておくこと。	◎				適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type II、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/従業員のライフサイクル、Amazon アカウントセキュリティ機能 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	・SOC1 Control Objectives2 Employee User Accessの基準に従った対策の実施。 ・PCI-DSS、SSAE16/ISAE3402の基準に従った対策の実施。 ・ISO 27001 管理策「アクセス制御／利用者パスワードの管理」に従った対策の実施。			●	2	AWSにより発行されたAWSアカウントを始め、各種管理者用アカウントのパスワード管理を行う。	-	-	-	-	○	-	-	-	-	-	-	-
A24100001	運18	V. 運用基準	運用管理(アクセス権限の管理)	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。	各種資源、システムへのアクセスを管理するため、アクセス権限を与えるにあたっての手続きを明確に定めることが必要である。さらに、アクセス権限を適切に保つため、見直しの手続きを明確化することが必要である。	◎				適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type II、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略、従業員のライフサイクル ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	・PCI-DSS、SSAE16/ISAE3402の基準に従った対策を実施。 ・ISO 27001管理策「アクセス制御／利用者アクセス権のレビュー」に従った対策の実施。			●	1	AWS上のシステム及びシステム運用上重要な情報へのアクセス権限の付与（見直しを含む）にあたっての手続きを明確にする。	-	-	-	-	-	-	-	-	-	-	-	-	-
A24300001	運19	V. 運用基準	運用管理(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。	コンピュータシステムの不正使用を防止するため、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のインラネットまたは他の情報処理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。	適合可能	○	公開情報	・AWS は、正式なポリシーと手順を確立し、AWS プラットフォームとインフラストラクチャホストに対する論理的なアクセスの、最低限の基準を定めてきました。	・Amazon Web Services: セキュリティプロセスの概要/従業員のライフサイクル				●	2	通常のシステム運用と同様に、システム運用のオペレーションにあたり、管理責任者が担当者の資格確認を行う。臨時処理や障害発生の際に、例外的に関係担当者等にオペレーション資格を付与する場合には、特に注意する。	-	-	-	-	-	-	△	-	-	-	-	-
A24400001	運20	V. 運用基準	運用管理(オペレーション管理)	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。	コンピュータシステムの不正使用を防止するため、オペレーションの依頼・承認手続きを明確にすること。	◎				適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type II、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001管理策「通信及び運用管理／運用の手順及び責任」に従った対策の実施。			●	1	通常のシステム運用と同様に、システム運用のオペレーションの依頼・承認手続きを明確にする。	-	-	-	-	-	-	-	-	-	-	-	-	-
A24500001	運21	V. 運用基準	運用管理(オペレーション管理)	運21 オペレーション実行体制を明確にすること。	コンピュータシステムの誤操作および不正使用を防止するため、オペレーション実行体制を明確にすること。	◎				適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type II、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001管理策「通信及び運用管理／運用の手順及び責任」に従った対策の実施。			●	1	通常のシステム運用と同様に、システム運用におけるオペレーションの体制と手順を明確にする。	-	-	-	-	-	-	-	-	-	-	-	-	-
A24600001	運22	V. 運用基準	運用管理(オペレーション管理)	運22 オペレーションの記録、確認を行うこと。	オペレーションの正 当性を検証するため、オペレーションの記録、確認を行うこと。	◎				適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type II、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001管理策「通信及び運用管理／監視に従った対策の実施。			●	2	通常のシステム運用と同様に、システム運用におけるオペレーション実行状況を確認する。また、依頼されたオペレーションが指示どおり処理されたことを確認できるよう、オペレーション記録を残す。具体的な方法としては、①AWS APIを用いて、オペレーションを手順化及び自動化したスクリプトを作成し、実行状況をログ出力する（ログの出力先は、システム運用PCや該当仮想マシンおよび別のAWSストレージサービス等がある）、②AWS Mangement Consoleの画面キャプチャを記録する等がある。	-	-	-	-	○	△	○	-	-	△	-	-	-
A24700001	運23	V. 運用基準	運用管理(オペレーション管理)	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。	クライアントサーバー・システムにおける不正使用等を防止するため、依頼、承認等の手続きを明確にし、実行、記録、結果確認等を適切に管理することが望ましい。	○				適合可能	—	—	—	—				●	2	（クライアント・サーバー型のシステムを導入する場合）通常のシステム運用と同様に、システム運用におけるオペレーション依頼、承認等の手続きを明確にし、実行、記録、結果確認等を適切に管理する。	-	-	-	-	-	△	○	-	-	-	-	-
A24900001	運24	V. 運用基準	運用管理(入力管理)	運24 データの入力管理を行うこと。	データの正確な処理と不正防止のため、入力手順を定めること。	◎			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。	適合可能	—	—	—	—				●	2	通常のシステム運用と同様に、データの入力手続き、承認等の手順を策定、実施する。	-	-	-	-	-	△	○	-	-	-	-	-
A25100001	運25	V. 運用基準	運用管理(データファイル管理)	運25 授受・保管理方法を定めること。	データファイルの不正使用、改ざん、紛失等を防止するため、データファイルの授受、保管は定められた方法によって行うこと。	◎			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。	適合可能	—	—	—	—				●	2	通常のシステム運用と同様に、データファイルの授受、保管方法を定め、実施する。	-	-	-	-	-	△	○	-	-	-	-	-
A25200001	運26	V. 運用基準	運用管理(データファイル管理)	運26 修正管理方法を明確にすること。	不正使用・改ざんを防止するため、データファイルに不整合が生じた場合のデータファイルの修正および管理は、定められた方法でおこなう。	◎			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。	適合可能	—	—	—	—				●	2	通常のシステム運用と同様に、データファイルの修正及び管理方法を定め、実施する。	-	-	-	-	-	△	○	-	-	-	-	-
A25300001	運27	V. 運用基準	運用管理(データファイル管理)	運27 バックアップを確保すること。	重要なデータファイルの障害や災害等への対応のため、バックアップを取得し、管理方法を明確にすること。	◎		□		適合可能	—	—	—	—				●	2	AWS上に格納された重要なデータファイルやAmazon マシンイメージ（AMI）のバックアップを取得し、管理方法を明確にする。バックアップデータの種別により、バックアップ先を自社システムのストレージにするか、AWS上のAmazon S3等のストレージにするか検討する。	-	-	-	-	○	△	○	-	△	-	○	-	-
A25500001	運28	V. 運用基準	運用管理(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。	プログラムの改ざん、破壊等を防止するため、プログラムファイルの管理は、定められた方法によって行うこと。	◎			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。	適合可能	—	—	—	—				●	2	通常のシステム運用と同様に、ゲストOS、ミドルウェア、アプリケーションのプログラムファイルの構成管理を実施する。	-	-	-	-	-	△	○	-	-	-	-	-
A25600001	運29	V. 運用基準	運用管理(プログラムファイル管理)	運29 バックアップを確保すること。	プログラムの障害や災害等への対応のため、バックアップを取得し、管理方法を明確にすること。	◎				適合可能	—	—	—	—				●	2	通常のシステム運用と同様に、構成管理の中でプログラムファイルのバックアップを実施する。	-	-	-	-	-	△	○	-	○	-	-	-	-
A25800001	運30	V. 運用基準	運用管理(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。	コンピュータウイルス等の侵入および感染に備えて、防御、検知、復旧の手順を明確にしておくこと。	◎			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、SOC2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証明されています。	適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type II0認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明				●	3	仮想マシン（ゲストOS）上でウィルス対策を実施する。ウィルスに感染した場合の復旧の手順を明確にする。	-	○	-	-	-	-	-	-	-	-	-	-	-

FISC 安対基準第8版および第8版追補からの引用									FISC安全対策基準に対するAWSの見解	FISC 安対基準への適合性	クラウド事業者の対応 (Amazon Web Services)							SI事業者・利用者で必要な対応			クラウド特有の対応方法 ○・・・対応必須、△・・・対応推奨																	
																						クラウドの一般的対応方法				AWS特有の対応方法													
																						実装			プロセス	実装												プロセス
SEQ	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	必須とされている項目	第8版追補での改訂	追108関連			対応状況	開示レベル	実施内容 （参照された内容等）	公開文章への参照	第三者認証から類推出来る内容	AWS/ADSJへのインタビュー結果	NDAベース資料への参照	対応要否	対応パターン	対策例	暗号化	Antivirus	FW/IDS/IPS	キー・署名の外部管理	証跡等の保管場所	API	IAM	VPC	Multi-AZ	CloudWatch (EC2)	EBS/Snapshot(EC2)	Auto Scaling (EC2)	ELB (EC2)	Management Cosole	Security Group	Direct Connect	AWSサポート
A26000001	運31	V. 運用基準	運用管理(ネットワーク及び情報管理)	運31 設定情報の管理を行うこと。	ネットワーク機器の設定情報が不正に変更されないように管理を行うこと。	○			AWSインフラストラクチャに対する脆弱性や非ルーチン作業を含む構成の変更については全てIT部門、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。	適合可能	○	詳細版に記載	–	–	・SOC1 Control Objectives3: Logical Security の基準に従った対策を実施。 ・SSAE16/ISAE3402の基準に従った対策を実施。			●	2	AWSのSecurity GroupやElastic Load Balancing(ELB)、Amazon VPC等でのネットワーク間通設定を管理する、ネットワーク間通設定を変更する際には、変更手続きを経たとで実施する、設定変更の際には、AWS Management Console等を用いて認証を行い、権限を持つ担当者のみが実施するものとする。	–	–	–	–	–	△	–	–	–	–	○	–	–	–
A26100001	運32	V. 運用基準	運用管理(ネットワーク及び情報管理)	運32 設定情報のバックアップを確保すること。	ネットワーク設定情報の不正な変更、障害や災害等への対応のため、バックアップを取得し、管理方法を明確にすること。	○				適合可能	○	詳細版に記載	–	–	–			●	2	AWS APIを用いて作成したスクリプト等により、Security GroupやElastic Load Balancing(ELB)等のネットワーク設定情報を収集し、バックアップを取得する。	–	–	–	–	○	△	–	–	–	–	–	–	–	–	–	–	–
A26300001	運33	V. 運用基準	運用管理(ドキュメント管理)	運33 保管管理方法を明確にすること。	不正使用、改ざん、紛失等を防止するため、ドキュメントは定められた方法によって管理すること。	○			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。 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、自然災害を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。	適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type II、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001管理策「通信及び運用管理/システム文書の セキュリティ」に従った対策の実施。			●	1	通常のシステム運用と同様に、システム運用に おける手順書等のドキュメントを保管管理する。	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A26400001	運34	V. 運用基準	運用管理(ドキュメント管理)	運34 バックアップを確保すること。	災害時の復旧対応のため、復旧に必要なドキュメントはバックアップを取得し、管理方法を明確にすること。	○				適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type II、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001管理策「通信及び運用管理/バックアップ」に従った対策の実施。			●	1	通常のシステム運用と同様に、災害時の復旧対応に必要なドキュメントは、バックアップを取得し、管理方法を明確にする。	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A26600001	運35	V. 運用基準	運用管理(帳簿管理)	運35 未使用重要帳票の管理方法を明確にすること。	不正使用を防止するため、未使用重要帳票の在庫管理および廃棄は定められた方法によって行うこと。	○			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。	適合可能	–	–	–	–	–			●	1	顧客データや取引情報等重要なデータを含む帳票を取り扱う場合は、未使用重要帳票の在庫管理および廃棄方法を明確にする。	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A26700001	運36	V. 運用基準	運用管理(帳票管理)	運36 重要な印字済帳票の取扱方法を明確にすること。	不正使用を防止するため、重要な印字済帳票の受渡しおよび廃棄は定められた方法によって行うこと。	○				適合可能	–	–	–	–	–			●	1	顧客データや取引情報等重要なデータを含む帳票を取り扱う場合は、印字済帳票の受渡し、保管、廃棄方法を明確にする。	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A26900001	運37	V. 運用基準	運用管理(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。	出力情報の改ざん、盗難、漏洩等を防止するため、作成、取扱い等にあたっては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。	適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type II、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001管理策「資産の管理/ 情報のラベル付け及び取扱い」に従った対策の実施。			●	1	通常のシステム運用と同様に、システム運用端末における出力情報、操作ログの漏洩対策を施す。	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A27100001	運38	V. 運用基準	運用管理(取引の管理)	運38 各取引の操作権限を明確にすること。	端末機操作による不正、不当取引を防止するため、取引内容ごとに端末機操作者等が操作できる権限の範囲を明確にすること。	○			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。	適合可能	–	–	–	–	–			●	1	通常のシステム運用と同様に、システム運用担当者に対する各取引の操作権限を範囲を明確にする。	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A27200001	運39	V. 運用基準	運用管理(取引の管理)	運39 オペレータカードの管理を行うこと。	端末機操作による不正取引を防止するため、オペレータカードは管理者を定め管理すること。	○				適合可能	–	–	–	–	–			●	1	通常のシステム運用と同様に、システム運用端末利用時の認証情報となるオペレータカード（ICカード等）は、管理者を定め管理する。	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A27300001	運40	V. 運用基準	運用管理(取引の管理)	運40 取引の操作内容を記録・検証すること。	端末機操作による不正取引を防止するため、取引明細表、端末機操作記録等により、取引内容が検証できる体制を整備すること。	○				適合可能	–	–	–	–	–			●	1	通常のシステム運用と同様に、システム運用端末で実施した操作のログを記録し、問題がないことを定期的に確認する。	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A27400001	運41	V. 運用基準	運用管理(取引の管理)	運41 顧客からの盗出の受付体制を整備し、事故口座の管理を行うこと。	事故による不正使用を防止するため、口座とリンクして顧客資産の移動を可能とする磁気および媒体の盗難等の届けを受け付けられる体制を整備すること。また、事故届のあった口座の管理は定められた方法により行うこと。	○				対象外	対象外	対象外						対象外																				
A27500001	運42	V. 運用基準	運用管理(取引の管理)	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。	利用者に責任と注意を喚起するため、電子的価値を蓄積する媒体および通信等に使用する機器の盗難、破損等に伴い、利用者が被る可能性がある損失および利用者側の責任についてもわかり易く明示すること。	○				適合可能	–	–	–	–	–			●	1	データを格納するストレージ等の盗難、破損等に伴い、利用者が被る可能性がある損失および利用者側の責任を契約書等でわかり易く明示する必要がある、システム運用側として、説明に必要な情報を提供する。	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A27700001	運43	V. 運用基準	運用管理(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。	不正行為を防止するため、暗号鍵の利用において暗号鍵の生成、配布、使用および保管等に係わる手続きを定めておくこと。また、その管理書類等は改廃者が厳重に管理すること。	○			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,Simple DB やEC2など、ほぼすべ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	適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type II、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001管理策「情報システムの取得、開発及び保守／暗号による管理策／かぎ（鍵）管理」に従った対策の実施。			●	1	データを暗号化する場合、暗号鍵の利用において暗号鍵のライフサイクル（生成、配布、使用および保管等）に係わる手続きを明確にする。	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A27900001	運44	V. 運用基準	運用管理(最正な本人確認の実施)	運44 本人確認を行うこと。	口座開設等を行う場合は適切な方法により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限を行なう事が出来、それらの管理は利用者の責任となります。	適合可能	–	–	–	–	–			●	1	インターネットバンキング等の非対面取引において、口座開設等を行う場合は、適切な方法により本人確認を行う仕組みをアプリケーションに実装する。	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A28000001	運44-1	V. 運用基準	運用管理(最正な本人確認の実施)	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。	不正払戻し防止のための措置を講ずることにより機械式預貯金払戻し等が正当な権限を有する者に対して適切に行われることを確保すること。	○				適合可能	–	–	–	–	–			●	1	CD・ATM等における正当な権限者の取引であることを確保する技術対策を取る必要があるが、システム運用としては、異常取引検知技術の導入等を検討する。	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A28200001	運45	V. 運用基準	運用管理(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。	CD・ATMおよび無人店舗の安全性を確保するため、円滑に稼動させるため、運用管理方法を明確に定めること。	○			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限を行なう事が出来、それらの管理は利用者の責任となります。	対象外	対象外	対象外	–	–	–			対象外																				
A28300001	運46	V. 運用基準	運用管理(CD・ATM等および無人店舗の管理)	運46 監視体制を明確にすること。	無人店舗における異常状態を発見するため、監視体制を明確にすること。	○				対象外	対象外	対象外	–	–	–			対象外																				
A28400001	運47	V. 運用基準	運用管理(CD・ATM等および無人店舗の管理)	運47 防犯体制を明確にすること。	無人店舗における犯罪を防止するため、防犯方法および犯罪発生時の対応方法を明確にすること。	○				対象外	対象外	対象外	–	–	–			対象外																				
A28500001	運48	V. 運用基準	運用管理(CD・ATM等および無人店舗の管理)	運48 障害時・災害時の対応方法を明確にすること。	無人店舗の円滑な運営のため、障害時・災害時の対応方法を明確にすること。	○				対象外	対象外	対象外	–	–	–			対象外																				
A28600001	運49	V. 運用基準	運用管理(CD・ATM等および無人店舗の管理)	運49 関係マニュアルの整備を行うこと。	無人店舗の円滑な運営、安全確保のため、各種対応を想定した関係マニュアルを整備しておくこと。	○				対象外	対象外	対象外	–	–	–			対象外																				
A28800001	運50	V. 運用基準	運用管理(渉外端末の管理)	運50 運用管理方法を明確にすること。	渉外端末の不正使用を防止するため、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。	適合可能	対象外	対象外	–	–	–			●	2	システム運用において、渉外端末にスマートデバイスを利用する場合は、(1)端末へのデータ保存、(2)MDMの導入、(3)紛失・盗難対策、(4)機種またはOSの選択、(5)通信機能の利用、(6)抗ウイルスソフト等について考慮する。	–	–	–	–	–	–	–	–	○	–	–	–
A29000001	運51	V. 運用基準	運用管理(カード管理)	運51 カードの管理方法を明確にすること。	安全性の確保および処理の円滑化のため、カードの発行、保管、交付、回収および廃棄は定められた方法によって行うこと。	○			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。	対象外	対象外	対象外	–	–	–			対象外																				
A29100001	運51-1	V. 運用基準	運用管理(カード管理)	運51-1 顧客に対して犯罪に関する注意喚起を行うこと。	顧客並びに取引の安全性を確保するため、犯罪に関する注意喚起を行うこと。	○				対象外	対象外	対象外	–	–	–			対象外																				
A29200001	運52	V. 運用基準	運用管理(カード管理)	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。	不正使用を防止するため、指定された口座のカード取引を監視できる方法を明確にすること	○				対象外	対象外	対象外	–	–	–			対象外																				
A29400001	運53	V. 運用基準	運用管理(顧客データ保護)	運53 顧客データの保護策を講ずること。	顧客データを保護し、適正に利用するため、管理・取扱い方法を定めること。	○			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。	適合可能	–	–	–	–	–			●	3	顧客に関する最低な守秘義務に基づき、顧客データの取扱いに関しては、管理責任者、管理方法および取扱い方法を定め適正に管理する。	○	–	–	○	–	–	–	–	–	–	–	–	–	–
A29500001	運53-1	V. 運用基準	運用管理(顧客データ保護)	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。	顧客を認証する手段として、生体認証を用いる場合に、生体認証情報を安全に管理するための手順を定めること。	○				適合可能	–	–	–	–	–			●	3	生体認証情報を取り扱う各段階(取得、入力、利用、保存、消去等)について、安全に管理するための手順を定める、各段階において、取扱者は必要最小限に限定する。	○	–	–	○	–	–	–	–	–	–	–	–	–	–
A29700001	運54	V. 運用基準	運用管理(資源管理)	運54 能力および使用状況の確認を行うこと。	コンピュータシステムの障害および処理能力の低下を回避するため、各種資源の能力および使用状況の確認を行い、適切な措置を講ずること。	○	■		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、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。	適合可能	○	詳細版に記載	–	–	–			●	2	コンピュータシステムの障害および処理能力の低下を回避するため、AWS Cloudwatchや等を利用して、能力および使用状況の確認を行う。また、使用状況確認結果を継続的に分析し、システムの性能強化や機能強化、組合せの再検討等を行う。	–	–	–	–	–	○	–	△	△	–	–	–
A29900001	運55	V. 運用基準	運用管理(外部接続管理)	運55 接続契約内容を明確にすること。	外部との接続を安全かつ正確に行うため、回線接続によるデータ授受に係わる契約締結にあたっては、接続の方法、データフォーマット、データ内容等を明確にすること。	○			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、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。	適合可能	–	–	–	–	–			●	1	通常のシステム運用と同様に、 回線接続によるデータ授受に係わる契約を締結するにあたっては、契約に盛り込まれた内容を十分把握し、損害賠等のないようにすることが必要である。このため、接続条件確認書を作成するなど標準化を図っておく。	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A30000001	運56	V. 運用基準	運用管理(外部接続管理)	運56 外部接続における運用管理方法を明確にすること。	データ漏洩、不正アクセス等を防止するため、外部接続時には運用管理方法を明確にし、相手先確認、接続条件(パスワード等)の登録・変更管理などを適切にけうこと。	○	■			適合可能	○	詳細版に記載	–	–	–			●	1	通常のシステム運用と同様に、 回線接続によりデータ授受を行う場合には、契約や定められた規定などにより接続相手先のネ入確認や端末確認の方法を明確にし、適切な管理を行う。	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A30200001	運57	V. 運用基準	運用管理(機器の管理)	運57 管理方法を明確にすること。	コンピュータシステムを構成する各種器の不正使用、破壊、盗難等を防止するため、定められた方法によって管理すること。	○	■		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、利用者の権限における管理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。	適合可能	○	詳細版に記載	–	–	–			●	2	機器については、管理責任者を明確にするとともに、関係者以外容易に接近できない、重要なサーバー等は、許可された人のみ操作ができるように する措置をとる。	–	–	–	–	–	○	–	–	–	–	–	–
A30300001	運58	V. 運用基準	運用管理(機器の管理)	運58 ネットワーク関連機器の保護措置を講ずること。	不正使用、破壊、盗難等を防止するため、重要なデータを扱うシステムを構成するネットワーク機器等は、適切な保護措置が講じられていることが望ましい。	○				適合可能	○	詳細版に記載	–	–	–			●	2	重要なデータを扱うシステムの場合、ルータやファイアウォール等のネットワーク機器に関しても不正使用、破壊、盗難等された場合の影響が大きい、このため、ネットワーク機器も、必要に応じてサーバー設置場所に準ずる機器管理を行う。	–	–	–	–	–	○	–	–	△	–	–	–
A30400001	運59	V. 運用基準	運用管理(機器の管理)	運59 保守方法を明確にすること。	コンピュータシステムを構成する各機器の障害を防止するため、保守点検を実施し、点検内容および結果を把握すること。	○				適合可能	○	詳細版に記載	–	–	–			–	–	–																	
A30600001	運60	V. 運用基準	運用管理(運行監視)	運60 監視体制を整備すること。	異常状態早期発見のため、監視対象、監視内容および監視方法を定めること。	○			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、監視手順を定義する責任があります。 AWS Cloudwatchはは 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 を参照してください。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を参照してください。	適合可能	○	公開情報	・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、アラーム設定されています。 ・Amazon CloudWatch は、Amazon EC2で起動し、AWSクラウドリソースのモニタリングを提供するウェブサービスです。	・Amazon Web Services: セキュリティプロセスの概要/モニタリング、Amazon CloudWatch のセキュリティ				●	2	システムの異常状態を早期発見するとともに、不正使用を発見、防止するため、AWS Cloudwatch等を利用して、監視体制を整備する。また、異常状態や不正使用を発見したときの対応方法を明確にしておく。	–	–	–	–	○	○	–	–	○	–	–	–	–	–
A30800001	運61	V. 運用基準	運用管理(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。	不法侵入、危険物持込み、不法持出し等を防止するため、コンピュータ室およびデータ保管室等重要な室における入室者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段階認証を経た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。定期的にけな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。	適合可能	○	詳細版に記載	–	–			–	–																				
A31000001	運62	V. 運用基準	運用管理(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。	障害時・災害時に関係者へ迅速かつ確実に連絡を行うため、連絡手順を定めておくこと。	○	■		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、自然災害を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 Security Whitepaperの第	適合可能	○	公開情報	・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。	・Amazon Web Services: セキュリティプロセスの概要/事業継続性管理				●	2	障害時・災害時に連絡を行い、招集する関係者をあらかじめ登用しておき、定期的に見直す。なお、災害時優先通信を含めた複数の連絡手段及び到達の必要性を明確にする。AWS内のサービス障害については、AWSやサポートが活用できる。特に、重大な障害、災害については、想定される最大リスク等を含め、経営層への報告フローを策定する。	–	–	–	–	–	–	–	–	–	–	–	–	–	△

FISC 安全対策基準第8版および第8版追補からの引用									FISC安全対策基準に対するAWSの見解	FISC 安対基準への適合性	クラウド事業者の対応 (Amazon Web Services)							SI事業者・利用者で必要な対応			クラウド特有の対応方法 ○・・・対応必須、△・・・対応推奨																			
																						クラウドの一般的対応方法					AWS特有の対応方法															
																						実装			プロセス		実装													プロセス
SEQ	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	必須とされている項目	第8版追補での改訂	追108関連			対応状況	開示レベル	実施内容（参照された内容等）	公開文書への参照	第三者認証から類推出来る内容	AWS/ADSJへのインタビュー結果	NDAベース資料への参照	対応要否	対応パターン	対策例	暗号化	Antivirus	FW/IDS/IPS	キー・署名の外部管理	証跡等の保管場所	API	IAM	VPC	Multi-AZ	CloudWatch (EC2)	EBS/Snap Shot(EC2)	Auto Scaling (EC2)	ELB (EC2)	Management Cosole	Security Group	Direct Connect	AWSサポート
A31100001	運63	V. 運用基準	運用管理(障害時・災害時対応策)	運63 障害時・災害時復旧手順を明確にすること。	障害または災害等によりコンピュータシステムが正常に稼働しなくなった場合の復旧手順を明確にすること。なお、当該手順については、コンティンジェンープランと整合性のとれた内容にすること。		■	□																															
A31200001	運64	V. 運用基準	運用管理(障害時・災害時対応策)	運64 障害の原因を調査・分析すること。	すばやく復旧するため、障害の原因を調査する手法を講じておくこと。また、障害の発生原因を記録し、傾向分析等を通じて再発防止に役立てること。	○	■				適合可能	○	詳細版に記載	—	—				●	2	障害時・災害時復旧手順を作成することで、障害または災害等により従来に稼働しなくなったコンピュータシステムを復旧させるための手順書を明確にする。併せて、バックアップシステムへの切り替え時の社内システムへの影響確認、切り戻しについて考慮する。 AWSでは、複数のアベイラビリティゾーンを利用した復旧も考慮する。	-	-	-	-	-	-	-	-	-	-	○	-	-	-	-	-	-	-	-
A31400001	運65	V. 運用基準	運用管理(コンティンジェンープランの策定)	運65 コンティンジェンープランを策定すること。	不慮の災害や事故、あるいは障害等により重大な損害を被り、業務の遂行が困難になった場合の損害の範囲と業務への影響を極小化し、早期復旧をはかるために、あらかじめコンティンジェンープラン（緊急時対応計画）を策定しておくこと。	○	■		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タイプ2、SOC2タイプ2レポートを参照して下さい。	適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type II/Pの認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要／コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス／AWS の認定とサードパーティによる証明				●	2	不慮の災害や事故、あるいは障害時に、あらかじめ想定される複数のケースに応じてコンティンジェンープランを策定しておく。コンティンジェンープランが策定された後においても、適宜見直しを行う。	-	-	-	-	○	-	△	△	△	-	-	-	-
A31700001	運66	V. 運用基準	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。	システムの導入、変更、廃棄を確実に行うため、ハードウェア、ソフトウェアの構成管理、版数管理などを行うこと。		○		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CMWS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	適合可能	○	公開情報	・既存のAWSインフラストラクチャに対する変更、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。	・Amazon Web Services: セキュリティプロセスの概要／設定管理				●	1	通常のシステム運用と同様に、 システム開発や導入時においては、下記項目について、考慮し把握していることが望ましい。 ・製品入手可能期間(販売終了予定日等) ・サポート期間(サポート終了予定日、サポート期間延長の可否) また、ハードウェア、ソフトウェアを適切に管理するため、台帳等を作成する。	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A31900001	運67	V. 運用基準	システム開発・変更（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。	システム開発・変更における内容の正当性を確保するため、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/	適合可能	—	—	—	—				●	1	通常のシステム運用と同様に、 システムの信頼性を向上させるとともに、内容の正当性を確保するため、システム開発・変更の各段階における確認、検証等は定められた手順によって行う。	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A32000001	運68	V. 運用基準	システム開発・変更（システム開発・変更管理）	運68 テスト環境を整備すること。	本番システムの安全性を確保するため、本番環境へ影響を与えないようなテスト環境を整備すること。		○	■		適合可能	—	—	—	—				●	1	通常のシステム運用と同様に、 システムの開発・変更作業に係わるテストにおいては、本番環境へ影響を与えずに十分なテストが実施する。なお、本番環境と開発環境はできる限り分離することが望ましい。	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A32100001	運69	V. 運用基準	システム開発・変更（システム開発・変更管理）	運69 本番への移行手順を明確にすること。	本番システムの安全性を確保するため、本番への移行に際しては、各システムの特性を考慮し、移行手順を明確にするとともに、関連する各部門の手順の整合性を確認すること。		○	■		適合可能	—	—	—	—				●	1	通常のシステム運用と同様に、 本番への移行は、移行時における障害を防止することが重要であり、本番システムへの切替えを安全・確実に行うためのシステムの特性に応じた移行手順を明確にする。また、月次な運用に移行するため、運用部門(運用担当者)への引継ぎ、説明およびユーザーへの説明を十分に行い、準備状況を確認する。	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A32300001	運70	V. 運用基準	システム開発・変更（ドキュメント管理）	運70 作成手順を定めること。	システムドキュメントを適切に作成するため、作成対象とするものを決め、それらについての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。 AWS利用者は、自身の開発、コンテンツ、運用、メンテナンスのドキュメントやその管理に対しての責任があります。	適合可能	○	公開情報	・ISO 27001の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要／コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス／AWS の認定とサードパーティによる証明				●	1	通常のシステム運用と同様に、 一貫した適切なドキュメントを作成するため、作成対象とするシステムドキュメントの範囲、体系、様式、記述内容等について明文化した手順を定め、遵守する。また、ドキュメントは、その品質を確認し、共有できるシステム資産とするために、作成部門および利用部門の責任者の承認を得ておく。	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A32400001	運71	V. 運用基準	システム開発・変更（ドキュメント管理）	運71 保管管理方法を明確にすること。	円滑な利用および改ざん、不正使用等の防止のため、システムドキュメントの保管管理を適正に行うこと。		○			適合可能	○	公開情報	・ISO 27001の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要／コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス／AWS の認定とサードパーティによる証明				●	1	通常のシステム運用と同様に、 ドキュメントの保管管理は、その利用を円滑にし、かつ不正使用防止や機密保護のために、定められた手順に従って適正に行う。	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A32600001	運72	V. 運用基準	システム開発・変更（パッケージの導入）	運72 評価体制を整備すること。	パッケージを導入する場合のシステム開発・変更を円滑に行うため、パッケージの有効性、信頼性、生産性等を評価する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。	適合可能	—	—	—	—				●	1	通常のシステム運用と同様に、 パッケージ導入に際しては、システム開発部門、運用部門および利用部門による総合的評価を行う。必要なカスタイズや特来の案件対応のために、パッケージのソースコード開示の可否を確認する。	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A32700001	運73	V. 運用基準	システム開発・変更（パッケージの導入）	運73 運用・管理体制を明確にすること。	パッケージの導入後のトラブル対応、機能拡張等を円滑に行うため、パッケージの運用・管理体制を明確にすること。		○			適合可能	—	—	—	—				●	1	通常のシステム運用と同様に、 パッケージ供給元の連絡窓口と保守体制および障害等作成手順や、ライセンス管理とバージョン管理体制等のパッケージの運用・管理体制を明確にする。	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A32900001	運74	V. 運用基準	システム開発・変更（システムの廃棄）	運74 廃棄計画、手順を策定すること。	システムの廃棄を円滑、確実かつ安全に実施するため、運用およびユーザー責任者の承認を得て不正防止、機密保護対策を含めた計画、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。	適合可能	○	公開情報	・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。	・Amazon Web Services: セキュリティプロセスの概要／ストレージデバイスの廃棄				●	3	システム廃棄にあたって機密保護等の措置を講じるために、利用者側としては、書籍データを暗号化するとともにサービス提供側のディスク廃棄時の情報漏洩対策を施すことができる。	○	-	-	○	○	-	-	-	-	-	-	-	-
A33000001	運75	V. 運用基準	システム開発・変更（システムの廃棄）	運75 情報漏洩防止対策を講ずること。	機密保護や不正防止等のため、システムの廃棄にあたっては機器等から情報漏洩が生じないように防止策を講ずること。		○	□	ISO27001規格に準じ、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。 「"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。	適合可能	○	公開情報	・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。	・Amazon Web Services: セキュリティプロセスの概要／ストレージデバイスの廃棄				●	3	内部の重要なデータを読み出し不可能とするために、利用者側としては、書籍データを暗号化するとともにサービス提供側のディスク廃棄時の情報漏洩対策を施すことができる。	○	-	-	○	○	-	-	-	-	-	-	-	-
A33300001	運76	V. 運用基準	各種設備管理(保守管理)	運76 管理方法を明確にすること。	コンピュータシステムを円滑に運用するため、設備の管理責任者および管理方法を明確にし、定められた方法によって管理すること。また、障害時・災害時の対応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	適合可能	○	公開情報	・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。	・Amazon Web Services: セキュリティプロセスの概要／設定管理				—	—	—	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A33400001	運77	V. 運用基準	各種設備管理(保守管理)	運77 保守方法を明確にすること。	コンピュータシステムを円滑に運用するため、保守点検を実施し、点検内容および結果を把握すること。		○			適合可能	○	公開情報	・既存のAWSインフラストラクチャに対する変更、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。	・Amazon Web Services: セキュリティプロセスの概要／設定管理				—	—	—	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A33600001	運78	V. 運用基準	各種設備管理(資源管理)	運78 能力および使用状況の確認を行うこと。	異常状態早期発見のため、各種設備の容量および性能の限界を把握し、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。	適合可能	○	詳細版に記載	—	—				—	—	—	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A33800001	運79	V. 運用基準	各種設備管理(監視)	運79 監視体制を整備すること。	異常状態早期発見のため、監視対象、監視内容および監視方法を定めること。		○		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	適合可能	○	公開情報	・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。 ・Amazon CloudWatch は、Amazon EC2で起動し、AWSクラウドリソースのモニタリングを提供するウェブサービスです。	・Amazon Web Services: セキュリティプロセスの概要／設定管理、Amazon CloudWatch のセキュリティ				—	—	—	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A34100001	運80	V. 運用基準	教育・訓練(教育・訓練)	運80 セキュリティ教育を行うこと。	セキュリティ意識の向上を図るため、全役職員(外部委員を含む)に対するセキュリティポリシーの周知徹底と、具体的なセキュリティ対策実施に関するセキュリティ教育を、担当する業務内容等を勘案のうえで行うこと。		○		AWSは、社員が各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表現、更たにデザ会議、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。 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	適合可能	○	公開情報	・AWS は、様々な手段や内部コミュニケーションをグローバルレベルで実施し、従業員が各自の役割と責任を理解するのを手助けして、重要なイベントや時宜にかなった方法で通知しました。	・Amazon Web Services: セキュリティプロセスの概要／情報と伝達				●	1	通常のシステム運用と同様に、 会社(もしくは組織)として定めた、セキュリティポリシーに関する教育を、セキュリティ関連文書(セキュリティポリシー(基本方針)、セキュリティスタンダード(自社の安全対策基準)、およびこれに基づいて作成されたマニュアルや手順書等)により行い、これらを理解させ、責任と義務および懲罰等について周知徹底を図る。教育・訓練は定期的、計画的に行う。	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A34200001	運81	V. 運用基準	教育・訓練(教育・訓練)	運81 要員に対するスキルアップ教育を行うこと。	システムとその開発対象となる適用業務に関する知識および技術の向上を図るための教育を、担当する業務内容等を勘案のうえで行うこと。		○			適合可能	○	公開情報	・ISO 27001の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要／コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス／AWS の認定とサードパーティによる証明	ISO 27001管理策「人的資源のセキュリティに従った対策の実施。			●	1	通常のシステム運用と同様に、 コンピュータシステムの開発、運用および利用に携わる要員(外部委員を含む)に対し、職種、職責、経験年数等を考慮した社内教育、社外教育を行う。	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A34300001	運82	V. 運用基準	教育・訓練(教育・訓練)	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。	コンピュータシステムに係わる通常時運用の円滑化および変革災事務処理に係わる端末機器の操作習熟のため、オペレーションの教育および訓練を行うこと。		○			適合可能	○	公開情報	・ISO 27001の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要／コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス／AWS の認定とサードパーティによる証明	ISO 27001管理策「人的資源のセキュリティに従った対策の実施。			●	1	通常のシステム運用と同様に、 コンピュータシステムに係わる通常時の運用においては、システム進行状況の的確な把握、正常・迅速な運用対応等を円滑に行うため、新人配属時、新機種導入時、ソフトウェア変更時等に、オペレーションの教育および訓練を行う。	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A34400001	運83	V. 運用基準	教育・訓練(教育・訓練)	運83 障害時・災害時に備えた教育・訓練を行うこと。	障害時・災害時に備えるため、コンピュータシステムの運用に係わるオペレーション等の教育・訓練を行うこと。		○	■	□	適合可能	○	公開情報	・当社は構造化された実行プロセスに従い、新人社員がAmazon のツール、プロセス、システム、ポリシーおよび手順を熟知できるよう教育を行っています。	・Amazon Web Services: リスクとコンプライアンス／AWS リスク および コンプライアンスプログラム	教育を定期的に実施。			●	1	通常のシステム運用と同様に、 障害時・災害時におけるコンピュータシステムの運用を円滑に行うため、障害時・災害時マニュアルおよびコンティンジェンープランに基づいたオペレーションの教育・訓練を定期的に行う。また、訓練結果については、システム進行状況の的確な把握、分析・評価のうえ、次回訓練およびコンティンジェンープランに反映する。	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A34500001	運84	V. 運用基準	教育・訓練(教育・訓練)	運84 防災・防犯訓練を行うこと。	非常時に備えて防災・防犯訓練を行うこと。		○	■		適合可能	○	詳細版に記載	—	—				●	1	通常のシステム運用と同様に、防災組織、防犯組織が十分機能するよう、非常時を想定した防災・防犯訓練を行う。ただし、実施困難な場合には、机上訓練によって訓練内容をレビューすることも有効である。なお、それにあたっては災害時緊急連絡を含めた複数の連絡手段及び訓練の必要性を明確にする。	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A34800001	運85	V. 運用基準	要員管理(要員管理)	運85 要員の人事管理を適切に行うこと。	システムの円滑な運用のため、要員の配置、交替等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	適合可能	○	公開情報	・AWS は、正式なポリシーと手順を確立し、AWS プラットフォームとインフラストラクチャホストに対する論理的アクセスの、最低限の基準を定めてきました。	・Amazon Web Services: セキュリティプロセスの概要／従業員のライフサイクル				●	1	通常のシステム運用と同様に、 コンピュータシステムの運用に携わる人員(パートタイマー、派遣等外部委員を含む)の配置、交替等は、スキル、経験年数、人事面接等とセキュリティおよび効率面を考慮して、適切に行う。	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A34900001	運86	V. 運用基準	要員管理(要員管理)	運86 要員の健康管理を行うこと。	作業環境の整備や定期的に健康診断を実施するなど要員の健康管理を適切に行うこと。		○			適合可能	○	詳細版に記載	—	—				●	1	通常のシステム運用と同様に、 コンピュータシステムの運用に携わる人員(パートタイマー、派遣等外部委員を含む)の健康管理は、要員の勤務体制、作業内容、コンピュータ室内の環境等を考慮して定期的な健康診断およびカウンセリングを行う。	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A35200001	運87	V. 運用基準	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、事前に目的や範囲等を明確にすることが必要である。	システムの開発や運用等で外部委託を行う場合は、事前に目的や範囲等を明確にすることが必要である。		○		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。	適合可能	○	詳細版に記載	—	—				●	1	— システムの開発や運用で外部委託を行う場合は、事前に目的や業務範囲、形式、期間、費用、リスクの管理方法、委託先の選定条件、外部委託に関する自社窓口と役割等を明確にすること。再委託先等となるクラウド事業者が選定条件を満たせるか確認する。	-	-	-	-	-	-	-	-	-	-	-	-	-	-

FISC 安全対策基準第8版および第8版追補からの引用									FISC安全対策基準に対するAWSの見解	FISC 安対基準への適合性	クラウド事業者の対応 (Amazon Web Services)							SI事業者・利用者で必要な対応			クラウド特有の対応方法 ○・・・対応必須、△・・・対応推奨																	
																					クラウドの一般的対応方法					AWS特有の対応方法													
																					実装			プロセス		実装											プロセス
SEQ	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	必須とされている項目	第8版追補での改訂	運108関連			対応状況	開示レベル	実施内容（参照された内容等）	公開文章への参照	第三者認証から類推出来る内容	AWS/ADSJへのインタビュー結果	NDAベース資料への参照	対応要否	対応パターン	対策例	暗号化	Antivirus	FW/IDS/IPS	キー・署名の外部管理	証跡等の保管場所	API	IAM	VPC	Multi-AZ	CloudWatch (EC2)	EBS/Snap Shot(EC2)	Auto Scaling (EC2)	ELB (EC2)	Management Cosole	Security Group	Direct Connect	AWSサポート
A35300001	運87-1	V. 運用基準	外部委託管理(外部委託に関する計画)	運87-1 外部委託先の選定手続き	外部委託先の選定に際しては手続きを明確にし、委託業者を客観的に評価すること。委託業者の決定にあたっては、責任者の承認を得ること。	❂		□			適合可能	○	詳細版に記載	–	–				●	1	委託業者を選定するにあたっては、選定手続きを明確にし、安定性(財務内容)や健全性、組織体制、信頼度および受託実績、技術レベル等についてお客委託先を客観的に評価して、委託業者の決定する。再委託先等となるクラウド事業者が選定条件を満たせるか確認する。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A35400001	運88	V. 運用基準	外部委託管理(外部委託に関する計画)	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。	安全性確保のため、機密保護、安全遂行等に関する項目を盛込んだ委託契約を締結すること。	❂	■	□			適合可能	○	詳細版に記載	–	–				●	1	外部委託した業務が安全に遂行されるために、機密保護や安全な業務の遂行等を契約上で外部委託先と締結するとともに、その契約の遵守状況を定期的に確認する。再委託先等となるクラウド事業者との管理境界、責任分界点を取り決め、かつ安全対策を確認の上、締結する。 また、利用者にてクラウドサービスを利用する業務のRTOを考慮し、サービス停止時を想定したDR等の対応策を講ずる。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A35600001	運89	V. 運用基準	外部委託管理(外部委託業務管理)	運89 外部委託先の要員に対するセキュリティ管理を適切に行うため、外部委託業務の内容や作業の範囲に応じて、セキュリティポリシーをはじめとした各種ルールの遵守を義務づけ、教育、監査を行うこと。	外部委託先の要員のセキュリティ管理を適切に行うため、外部委託業務の内容や作業の範囲に応じて、セキュリティポリシーをはじめとした各種ルールの遵守を義務づけ、教育、監査を行うこと。	❂			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。		適合可能	○	詳細版に記載	–	–				●	1	外部委託先の要員が委託業務を遂行するにあたっては、金融機関等のセキュリティポリシーをはじめとした、外部委託先の要員が遵守すべきルールを委託業務の内容に応じて明確にし、これを遵守させる。再委託先等となるクラウド事業者の遵守状況を確認する。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A35700001	運90	V. 運用基準	外部委託管理(外部委託業務管理)	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。	外部に委託した業務内容を確認するため、業務組織の整備を行うとともに、委託契約に基づき管理、検証を行うこと。	❂	■	□			適合可能	○	詳細版に記載	–	–				●	1	金融機関等が外部委託した業務が安全に遂行されるために、機密保護や安全な業務の遂行等を契約上で外部委託先と締結するとともに、その契約の遵守状況を定期的に確認する。再委託先等となるクラウド事業者の管理状況を確認する。また、経営者が利用しているクラウドサービスを理解した上で、リスク・対策を把握・判断できるようシステム監査、モニタリングを実施する。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A35800001	運90-1	V. 運用基準	外部委託管理(外部委託業務管理)	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。	金融機関相互のシステム・ネットワークは、金融機関相互の金融取引の決済やCD/ATMオンライン提携などを行うため、基幹インフラとしての機能を担っている。仮にシステム・ネットワークにおいて、障害が発生した場合は、その影響は決済システム全体および顧客サービス全般に及ぼかねないことから、適切なリスク管理を行うこと。	❂					対象外	対象外	対象外	–	–				対象外																					
A36100001	運91	V. 運用基準	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。	コンピュータシステムおよびその管理について、有効性、効率性、信頼性、遵守性、および安全性の面から把握、評価するため、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。		適合可能	○	詳細版に記載	–	–				●	2	通常のシステム運用と同様に、 コンピュータシステムの運用、システム開発・変更等においては、コンピュータシステムの有効性、効率性、信頼性、遵守性、および安全性を確保するため、コンピュータ部門から独立したシステム監査人がシステムの総合的な監査・評価を行い、経営層に監査結果を報告する。 また、委託先経由でAWSプレミアムサポート(エンタープライズ)への監査内容の確認や内部監査部門による監査内容の確認を行う。	–	–	–	–	○	–	–	–	–	–	–	–	–	–	–	–	–	△
A36300001	運92	V. 運用基準	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。	インストアブランチの安全性を確保するため、出店先地域やストアの選定基準を明確にすること。	○					対象外	対象外	対象外	–	–				対象外																				
A36500001	運93	V. 運用基準	コンビニATM	運93 出店先の選定基準を明確にすること。	コンビニATMおよび利用者の安全性を確保するため、出店先地域やコンビニエンスストアの選定基準を明確にすること。	○					対象外	対象外	対象外	–	–				対象外																				
A36600001	運94	V. 運用基準	コンビニATM	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。	コンビニATMのメンテナンス時の安全性を確保するため、防犯体制および防犯方法を明確にすること。	○					対象外	対象外	対象外	–	–				対象外																				
A36700001	運95	V. 運用基準	コンビニATM	運95 障害時・災害時対応手順を明確にすること。	コンビニATMの障害時・災害時に迅速な対応を行うため、その対応手順を明確にすること。	○					対象外	対象外	対象外	–	–				対象外																				
A36800001	運96	V. 運用基準	コンビニATM	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。	伝送データの安全性、信頼性を確保し、また不正使用、破壊、改ざん等を防止するため、ネットワーク関連機器の適切な保護措置および伝送データの安全対策を講ずること。	○					対象外	対象外	対象外	–	–				対象外																				
A36900001	運97	V. 運用基準	コンビニATM	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。	犯罪発生時に関係者へ迅速に連絡を行うため、所轄の警察および警備会社等関係者との連絡体制の確立および訓練を行うこと。	○					対象外	対象外	対象外	–	–				対象外																				
A37000001	運98	V. 運用基準	コンビニATM	運98 顧客に対して犯罪に関する注意喚起を行うこと。	顧客ならびに取引の安全性を確保するため、犯罪に関する注意喚起を行うこと。	○					対象外	対象外	対象外	–	–				対象外																				
A37300001	運99	V. 運用基準	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。	デビットカード・サービスの安全性を確保するため、金融機関等はサービスの提供形態に応じて、情報処理センターや加盟店等と共に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ト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。		対象外	対象外	対象外	–	–				対象外																				
A37400001	運100	V. 運用基準	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100 口座番号、暗証番号等の安全性を確保すること。	口座番号、暗証番号等の安全性を確保するため、金融機関等はサービスの提供形態に応じて、情報処理センターや加盟店等と共に安全対策を講ずること。	○					対象外	対象外	対象外	–	–				対象外																				
A37600001	運101	V. 運用基準	デビットカード(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。	デビットカード利用時の安全性を確保するため、適切な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。		対象外	対象外	対象外	–	–				対象外																				
A37800001	運102	V. 運用基準	デビットカード(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。	顧客に注意を喚起するため、デビットカード利用上の留意事項を顧客に明示すること。	○					対象外	対象外	対象外	–	–				対象外																				
A38100001	運103	V. 運用基準	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。	オープンネットワークを利用した金融サービスの安全性を確保するため、接続相手先が本人であることを確認する予防策やアクセス制限、検知策等の不正使用防止機能を設けること。	❂	■		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。		適合可能	–	–	–	–				●	2	不正使用を防止するために、VPCによりインターネットへのアクセス制限しリスクを低減する。また、IAMを活用し厳正な本人確認も実施する。	–	–	△	–	–	–	○	–	–	–	–	–	–	△	–	–
A38200001	運104	V. 運用基準	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104 不正使用を早期発見すること。	利用者を不正使用から守るため、利用者自身が使用状態を確認する機能を設けること。	❂					適合可能	–	–	–	–				●	3	通常のシステム同様に、 利用者自身によりユーザーID等の不正使用の発見可能なFW/IDS/IPSや証跡保管等の手段を提供する。ただし、クラウドにおいては物理サーバへ直接アクセスができない場合があるため、証跡等の外部保管を考慮すること。	–	–	○	–	○	–	–	–	–	–	–	–	–	–	–	–	–
A38300001	運105	V. 運用基準	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105 安全対策に関する情報開示をすること。	利用者が適切に取引機関や金融サービスの選択を行うため、安全対策に関する情報を開示することが望ましい。	○					適合可能	–	–	–	–				●	3	通常のシステム同様に、 情報漏洩防止のために暗号化方法や、なりすまし防止のための認証方法等のセキュリティ方針等を開示するが、キー・署名については外部保管および管理していることを明確にする。	○	–	–	○	–	–	–	–	–	–	–	–	–	–	–	–	–
A38400001	運105-1	V. 運用基準	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105-1 顧客対応方法を明確にすること。	インターネット、モバイル等を用いた金融サービスにおいて、注意喚起や受付対応等の顧客対応方法を明確にすること。	❂	■				適合可能	–	–	–	–				●	1	通常のシステム運用と同様に、 注意喚起や受付対応等の顧客対応方法において、正当なサイトであること、正当なメールであることの確認手段 にも留意する。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A38500001	運106	V. 運用基準	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。	インターネットやモバイル等を用いた金融サービスにおいて、利用者を保護し、安全性を確保し円滑に稼働させるため、運用管理方法を明確化すること。	❂					適合可能	–	–	–	–				●	3	通常のシステム運用と同様に、 不正な取引を防止する対策について、本人確認機能、アクセス履歴の管理をとることができるが、証跡の重要度により外部保管も必要である。	–	–	–	–	○	–	–	–	–	–	–	–	–	–	–	–	–
A38700001	運107	V. 運用基準	オープンネットワークを利用した金融サービス(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。	電子メールの運用に当たっては、信頼性、安全性を確保するため、そ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。		適合可能	–	–	–	–				●	3	通常のシステム運用と同様に、 電子メールを盗聴およびなりすましや情報漏洩に利用される可能性があるため、暗号化、電子署名を活用する。	○	–	–	○	–	–	–	–	–	–	–	–	–	–	–	–	–
	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にあたっては、適切なリスク管理を行うこと。	クラウドサービスの利用は外部委託に相当すると認識し、適切なリスク管理を行うこと。	❂	■	□			適合可能	○		別途、シート「セキュリティリファレンス(運108関連)」を参照のこと。					●		別途、シート「セキュリティリファレンス(運108関連)」を参照のこと。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A39300001	技1	VI. 技術基準 I.システム信頼性向上対策	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。	ハードウェアの障害を予防するため、装置の特性や重要度に応じ、予防保守を定期的にまたは随時実施すること。	❂			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		適合可能	○	公開情報	・新しいハードウェアがプロビジョニングされると、内部開発された設定管理ソフトウェアがインストールされます。	・Amazon Web Services: セキュリティプロセスの概要/設定管理	ISO 27001の管理策には、「装置のセキュリティ」がある。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A39500001	技2	VI. 技術基準 I. システム信頼性向上対策	ハードウェアの信頼性向上対策(ハードウェアの予備)	技2 本体装置の予備を設けること。	本体装置の障害時に迅速に対応するため、重要な本体装置には予備を設けること。	❂	■		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(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やフィラには影響のあるエリアから遮断されます。AWS SOC1タイプ2、SOC2タイプIIレポートにはか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。		適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type IIの認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001の管理策には、「装置のセキュリティ」がある。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A39600001	技3	VI. 技術基準 I. システム信頼性向上対策	ハードウェアの信頼性向上対策(ハードウェアの予備)	技3 周辺装置の予備を設けること。	周辺装置の障害時に迅速な対応を行うため、重要な周辺装置は予備または代替機能を設けること。	❂	■				適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type IIの認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001の管理策には、「装置のセキュリティ」がある。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A39700001	技4	VI. 技術基準 I. システム信頼性向上対策	ハードウェアの信頼性向上対策(ハードウェアの予備)	技4 通信系装置の予備を設けること。	通信系装置の障害時の迅速な対応のために、重要な通信系装置は予備を設けること。	❂	■				適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type IIの認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001の管理策には、「装置のセキュリティ」がある。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A39800001	技5	VI. 技術基準 I. システム信頼性向上対策	ハードウェアの信頼性向上対策(ハードウェアの予備)	技5 回線の予備を設けること。	回線障害時の迅速な対応のために、重要な回線は予備を設けることが望ましい。	○	■				適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type IIの認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001の管理策には、「装置のセキュリティ」がある。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A39900001	技6	VI. 技術基準 I. システム信頼性向上対策	ハードウェアの信頼性向上対策(ハードウェアの予備)	技6 端末系装置の予備を設けること。	端末系装置の障害時の迅速な対応のために、端末系装置は予備または代替機能を設けること。	❂	■				適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type IIの認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001の管理策には、「装置のセキュリティ」がある。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A40200001	技7	VI. 技術基準 I. システム信頼性向上対策(開発時の品質向上対策)	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。	コンピュータシステム全体の信頼性向上のため、システム開発計画は、中長期のシステム化計画と整合性が取れており、かつ将来の技術調査を実施していること。また開発責任者(システム)を企画、開発する部門の長)の承認を得ていること。	❂	■		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・承認およ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		適合可能	○	公開情報	・AWS の開発プロセスは、安全なソフトウェア開発のベストプラクティスに従っており、これにはAWS セキュリティによる公式の設計レビュー、脅威のモデリング、リスクアセスメントの完遂などが含まれています。AWSでは、ELB、Route53(DNS)にてIPv6に対応しています。	・Amazon Web Services: セキュリティプロセスの概要/セキュリティ設計の原則		–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

FISC 安対基準第8版および第8版追補からの引用									FISC安全対策基準に対するAWSの見解	FISC 安対基準への適合性	クラウド事業者の対応 (Amazon Web Services)							SI事業者・利用者で必要な対応			クラウド特有の対応方法 ○・・・対応必須、△・・・対応推奨																	
																						クラウドの一般的対応方法			AWS特有の対応方法														
																						実装		プロセス	実装												プロセス
SEQ	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	必須とされている項目	第8版追補での改訂	追108関連			対応状況	開示レベル	実施内容（参照された内容等）	公開文書への参照	第三者認証から照推出来る内容	AWS/ADSJへのインタビュー結果	NDAベース資料への参照	対応要否	対応パターン	対策例	暗号化	Antivirus	FW/IDS/IPS	キー・署名の外部管理	証跡等の保管場所	API	IAM	VPC	Multi-AZ	CloudWatch (EC2)	EBS/Snap Shot(EC2)	Auto Scaling (EC2)	ELB (EC2)	Management Cosole	Security Group	Direct Connect	AWSサポート
A40300001	技8	VI. 技術基準 I. システム信頼性向上対策	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8 必要となるセキュリティ機能を取り込むこと。	セキュリティ対策を確実に実施するため、システム計画段階において必要となるセキュリティ機能が取り込まれていることを明確にすること。	◎					適合可能	○	公開情報	・AWS の開発プロセスは、安全なソフトウェア開発のベストプラクティスに従っており、これには AWS セキュリティによる公式の設計レビュー、脅威のモデリング、リスクアセスメントの完遂などが含まれています。	・Amazon Web Services: セキュリティプロセスの概要 / セキュリティ設計の原則	ISO 27001の管理策には、「情報システムの取得、開発及び保守」がある。			●	3	クラウドにおいては、暗号化と証跡等の保管をどのように行うかが重要となる。その際、機能、技術の選択において、計画段階から処理する業務やデータの重要性と処理する業務やデータのリスクを考慮し、暗号化の方式や証跡等の外部保管の場所・管理方法を考慮する。	○	–	–	–	○	–	–	–	–	–	–	–	–	–	–	–
A40400001	技9	VI. 技術基準 I. システム信頼性向上対策	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9 設計段階でのソフトウェアの品質を確保すること。	設計段階でのソフトウェアの信頼性向上のため、開発の前提となる要件を明確にするとともに、信頼度設計の考慮や設計作業の標準化等を行い、ソフトウェアの品質を確保すること。	◎	■				適合可能	○	公開情報	・AWS の開発プロセスは、安全なソフトウェア開発のベストプラクティスに従っており、これには AWS セキュリティによる公式の設計レビュー、脅威のモデリング、リスクアセスメントの完遂などが含まれています。	・Amazon Web Services: セキュリティプロセスの概要 / セキュリティ設計の原則	ISO 27001の管理策には、「情報システムの取得、開発及び保守」がある。			●	2	ソフトウェアの品質を確保するため、設計段階から品質を高めるために、次に留意する。 (1) 暗号化等のクラウドで特に必要とされるセキュリティ機能の組込み (2) 品質向上のためにCloudWatchによる監視や証跡等を保管する。 また、AWSにおいてはAPIを使用した機能の組み込みも可能であることに留意する。	△	–	–	–	○	○	–	–	–	–	–	–	–	○
A40500001	技10	VI. 技術基準 I. システム信頼性向上対策	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10 プログラム作成段階での品質を確保すること。	プログラム作成段階での、ソフトウェアの信頼性向上のため、プログラム仕様書に基づいたプログラミング名行うとともにプログラム作成作業の標準化・自動化等を行い、ソフトウェアの品質を確保すること。	◎	■				適合可能	○	公開情報	・AWS の開発プロセスは、安全なソフトウェア開発のベストプラクティスに従っており、これには AWS セキュリティによる公式の設計レビュー、脅威のモデリング、リスクアセスメントの完遂などが含まれています。	・Amazon Web Services: セキュリティプロセスの概要 / セキュリティ設計の原則	ISO 27001の管理策には、「情報システムの取得、開発及び保守」がある。			●	2	プログラムの作成段階において、APIを使用しソフトウェアの品質を確保できる。具体的な標準化・自動化として、次の方法がある。 (1) 適切な言語の選択 (2) 部品化、パターン化の有効活用	–	–	–	–	–	○	–	–	–	–	–	–	–	–
A40600001	技11	VI. 技術基準 I. システム信頼性向上対策	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11 テスト段階でのソフトウェアの品質を確保すること。	テスト段階でのソフトウェアの信頼性向上のために、テスト計画の策定、テスト環境・体制の整備、テストサポート機能の活用、テスト実施段階での各種管理等を行い、ソフトウェアの品質を確保すること。	◎	■				適合可能	○	公開情報	・AWS の開発プロセスは、安全なソフトウェア開発のベストプラクティスに従っており、これには AWS セキュリティによる公式の設計レビュー、脅威のモデリング、リスクアセスメントの完遂などが含まれています。	・Amazon Web Services: セキュリティプロセスの概要 / セキュリティ設計の原則	ISO 27001の管理策には、「情報システムの取得、開発及び保守」がある。			●	1	ソフトウェアの品質を確保するために、次のような事項に留意する。 (1) テスト計画書の作成 (2) テスト体制の整備 (3) テスト工程の分担 (4) 各種テストツールの活用	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A40700001	技12	VI. 技術基準 I. システム信頼性向上対策	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。	配布時のソフトウェアの信頼性を確保するため、配布先の稼働環境との整合性確認やウイルスチェックを行うこと。	◎					適合可能	–	–	–	–	–			●	3	プログラムを配布する際は、開発環境と、稼働環境の整合性を確認する。具体的な考慮事項には、次のものがある。 (1) ハードウェア環境 (2) OS、ミドルソフト等、それらのバージョン	–	○	–	–	–	–	–	–	–	–	–	–	–	–
A40800001	技13	VI. 技術基準 I. システム信頼性向上対策	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。	パッケージソフトウェアの品質を確保するために、機能およびシステムとの整合性を十分確認すること。	◎					適合可能	–	–	–	–	–			●	1	業務システムパッケージ導入時には品質を確保する。具体的には、次のものがある。 (1) パッケージ導入の前提となる要件の明確化 (2) 機能について記載された仕様書、設計書、テスト確認書等のドキュメントの確保	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A41000001	技14	VI. 技術基準 I. システム信頼性向上対策	ソフトウェアの信頼性向上対策(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。	営業店新設、機器増設等の定型的変更作業時における正確性を確保するため、変更作業の合理化等の必要な対策を講ずること。	◎			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。		適合可能	–	–	–	–	–			●	1	変更作業時においては、正確性を確保する。具体的には、次の方法がある。 (1) 変更作業の合理化 (2) 変更内容と作業手順のドキュメント化 (3) テストおよび検証手順の確立	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A41100001	技15	VI. 技術基準 I. システム信頼性向上対策	ソフトウェアの信頼性向上対策(メンテナンス時の品質向上対策)	技15 機能の変更、追加作業時の品質を確保すること。	機能の変更、追加作業時におけるソフトウェアの品質を確保するため、開発時の品質向上対策を準用すること。	◎					適合可能	–	–	–	–	–			●	2	機能の変更、追加における他への影響を確認し、極小化する。具体的には、次の方法がある。 (1) 変更、追加箇所の確認 (2) 影響度の検証 (3) 機能の変更、追加作業時の障害対策	–	–	–	○	○	○	–	–	–	–	–	–	–	–
A41400001	技16	VI. 技術基準 I. システム信頼性向上対策	運用時の信頼性向上対策(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。	オペレーションの信頼性を向上させるため、オペレーションの自動化、簡略化を図ることが望ましい。		○		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。		適合可能	○	詳細版に記載	–	–	–	–			●	2	コンピュータセンターでのオペレーションの自動化方法として、具体的には、次の方法がある。 (1) システムの起動を自動的に行う機能 (2) ジョブの起動やジョブと記憶装置の対応 (3) 各種自動運転機能 自動化を実現する手段としてAPIによる機能作成があることも留意する。	–	–	–	–	–	○	–	–	–	–	–	–	–	–
A41500001	技17	VI. 技術基準 I. システム信頼性向上対策	運用時の信頼性向上対策(運用時の信頼性向上対策)	技17 オペレーションのチェック機能を充実すること。	オペレーションミスを防止するため、チェック機能を充実すること。	◎					適合可能	○	詳細版に記載	–	–	–	–			●	2	コンピュータセンターにおいてオペレータの作業を確認するは、具体的に、次の方法がある。 (1) コマンド入力の再確認機能 (2) 妥当性チェック機能 (3) テープ使用時のラベルチェック機能 自動化を実現する手段としてAPIによる機能作成があることも留意する。	–	–	–	–	–	○	–	–	–	–	–	–	–	–
A41600001	技18	VI. 技術基準 I. システム信頼性向上対策	運用時の信頼性向上対策(運用時の信頼性向上対策)	技18 負荷状態の監視制御機能を充実すること。	コンピュータシステムの安定稼働のために、各種資源の能力や容量などの限界を超えないように負荷状態を監視し、必要に応じて制御する機能を充実すること。	◎					適合可能	○	公開情報	・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。	・Amazon Web Services: セキュリティプロセスの概要 / モニタリング	ISO 27001の管理策には、「通信及び運用管理」がある。			●	2	負荷状態の監視制御機能としては、具体的に、次の方法がある。 (1) 負荷状態表示機能 (2) 使用状況照会機能 (3) 統計分析機能 既定で提供されるCloudWatch以外に自動化を実現する手段としてAPIによる機能作成があることも留意する。	–	–	–	–	○	–	–	–	–	–	–	–	–	–
A41700001	技19	VI. 技術基準 I. システム信頼性向上対策	運用時の信頼性向上対策(運用時の信頼性向上対策)	技19 CD・ATM等の遠隔制御機能を設けること。	無人店舗におけるCD・ATM等の安定運用のために、運用状況を集中監視し、必要に応じて遠隔制御を行う機能を設けること。	◎					対象外	対象外	対象外	–	–	–			対象外																		
A42000001	技20	VI. 技術基準 I. システム信頼性向上対策	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。	障害の早期発見・回復のために、コンピュータシステムの運用状況(稼働状態、停止状態、エラー状態)を監視する機能を設けること。	◎			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、それらのシステムの状態を詳細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。			適合可能	○	公開情報	・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。 ・Amazon CloudWatch は、Amazon EC2で起動し、AWSクラウドリソースのモニタリングを提供するウェブサービスです。 ・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。	・Amazon Web Services: セキュリティプロセスの概要 / モニタリング、Amazon CloudWatch のセキュリティ、設定管理	ISO 27001の管理策には、「通信及び運用管理」がある。			●	2	監視の方法としては、具体的に、次の方法がある。 (1) ソフトウェアによる監視 (2) コンソールからのステータスディスプレイ機能による表示 (3) 遠隔監視盤等によるリモート監視 (4) サービスプロセッサによる監視 既定で提供されるCloudWatch以外に自動化を実現する手段としてAPIによる機能作成があることも留意する。	–	–	–	–	○	–	–	–	–	–	–	–	–	–
A42100001	技21	VI. 技術基準 I. システム信頼性向上対策	障害の早期発見・早期回復(障害の早期発見)	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。	迅速な障害回復に役立てるため、コンピュータシステムに発生する各種障害を的確に検出し、障害箇所を切り分ける機能を設けること。	◎					適合可能	○	公開情報	・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。 ・Amazon CloudWatch は、Amazon EC2で起動し、AWSクラウドリソースのモニタリングを提供するウェブサービスです。 ・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。	・Amazon Web Services: セキュリティプロセスの概要 / モニタリング、Amazon CloudWatch のセキュリティ、設定管理	ISO 27001の管理策には、「通信及び運用管理」がある。			●	2	障害を検出し、障害箇所の切り分けを行うための方法としては、具体的に、次の方法がある。 (1) 異常検出機能 (2) ロギング機能 (3) テスト機能 既定で提供されるCloudWatch以外に自動化を実現する手段としてAPIによる機能作成があることも留意する。	–	–	–	–	–	○	–	–	–	–	–	–	–	–
A42300001	技22	VI. 技術基準 I. システム信頼性向上対策	障害の早期発見・早期回復(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。	障害時に、一部の処理を中断しても、システム全体を停止させることなく運転を続行させるため、機能を縮小し、システムを再構成する機能を設けること。	◎			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ー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。複数のアベイラビリティー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ーゾーンを活かしたAWSの使用法を設計することが推奨されます。			適合可能	○	公開情報	・データセンターは、世界各地に複数構築されています。	・Amazon Web Services: セキュリティプロセスの概要 / 事業継続性管理 ※関連 Amazon Web Services: セキュリティプロセスの概要 / 障害分離	ISO 27001の管理策には、「通信及び運用管理」がある。			●	2	縮退・再構成機能として、具体的には、次の方法がある。 (1) 障害が発生した部分に関する取引を閉塞する機能 (2) 障害が発生した部分の切離しを行う機能 (3) 正常な構成要素で運転が続行できるように構成なおす機能	–	–	–	–	–	○	–	–	○	○	–	–	–	–
A42400001	技23	VI. 技術基準 I. システム信頼性向上対策	障害の早期発見・早期回復(障害の早期回復)	技23 取引制限機能を設けること。	ファイル障害やプログラミスス等による影響を極小化するため、ファイル単位、科目単位等による取引制限機能を設けること。	◎					適合可能	–	–	–	–	–			●	2	障害の影響を局所化することが必要であり、そのために、障害の状況に応じ障害箇所を、稼働中のシステムから切り離すなどの措置がとれるような機能を設ける。	–	–	–	–	–	△	–	–	–	△	–	–	–	–
A42500001	技24	VI. 技術基準 I. システム信頼性向上対策	障害の早期発見・早期回復(障害の早期回復)	技24 リカバリ機能を設けること。	障害が発生した場合は、速やかにシステムを回復させ業務を支障なく続行させるために必要なリカバリ機能を設けること。	◎					適合可能	–	–	–	–	–			●	2	リカバリ機能としては、具体的には、次の方法がある。 (1) リカバリ用ジャーナル機能 (2) チェックポイント機能 (3) 部分リカバリ機能	–	–	–	–	–	–	○	–	–	–	–	–	–	–
A42800001	技25	VI. 技術基準 I. システム信頼性向上対策	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。	コンピュータセンター等が災害等により機能しなくなった場合に備えて、業務の優先度を考慮してバックアップサイトを保有することが望ましい。		○	■			適合可能	○	公開情報	・Amazon S3、Amazon SimpleDB、または Amazon Elastic Block Store(EBS)に保存されるデータは、これらのサービスの通常操作の一部として、複数の物理的ロケーションで冗長的に保存されます。	・Amazon Web Services: セキュリティプロセスの概要 / バックアップ ※関連 Amazon Web Services: セキュリティプロセスの概要 / 障害分離				●	2	マルチAvailable Zone または、グローバルにマルチリージョンを構成することで、バックアップサイトを準備する。	–	–	–	–	–	○	–	○	–	○	–	–	–	–
A43200001	技26	VI. 技術基準 II. 安全性検査対策	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。	暗証番号・パスワード等の漏洩防止のため、表示、非印字等の必要な対策を講ずること。	◎			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、仮想ゼファ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外部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			適合可能	○	公開情報	・ISO 27001を始め、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要 / コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス / AWS の認定とサードパーティによる証明	ISO 27001の管理策には、「アクセス制御」がある。			●	2	暗証番号・パスワードの利用等にあたっての安全対策上の機能として、具体的には、次の方法がある。 (1) 暗証番号・パスワードにはNULLまたは少ない桁数を認めない機能 (2) 暗証番号・パスワードの使用に有効期間を設定し、有効期限近接時は、事前に変更要求を行う機能	○	–	–	○	–	–	○	–	–	–	–	–	○	–
A43300001	技27	VI. 技術基準 II. 安全性検査対策	データ保護(漏洩防止)	技27 相手端末確認機能を設けること。	公衆通信網を通じて自動着信端末に出力する場合には、誤接続を防止するため、確認可能なものについては相手端末を確認する機能を設けることが望ましい。		○				適合可能	○	公開情報	・ISO 27001を始め、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要 / コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス / AWS の認定とサードパーティによる証明				●	1	接続相手端末確認としては、具体的には、次の方法がある。 (1) 電話の発信者情報通知サービス、携帯電話の識別番号等の利用 (2) ファクシミリの端末ID の利用 (3) 認証機関が発行する電子的な証明書	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A43400001	技28	VI. 技術基準 II. 安全性検査対策	データ保護(漏洩防止)	技28 蓄積データの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が望ましい。		○				適合可能	○	公開情報	・ISO 27001を始め、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要 / コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス / AWS の認定とサードパーティによる証明				●	3	パスワード設定としては、具体的には、次の方法がある。 (1) データベース：DBMSの備えるパスワード (2) 文書ファイル：文書そのものにかけるパスワード (3) ハードディスク：ハードディスクドライブにかけるパスワード	○	–	–	–	–	–	–	–	–	–	–	–	–	–
A43500001	技29	VI. 技術基準 II. 安全性検査対策	データ保護(漏洩防止)	技29 伝送データの漏洩防止策を講ずること。	データ伝送時の盗聴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の対策を講ずることが望ましい。		○	■			適合可能	○	公開情報	・ISO 27001を始め、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要 / コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス / AWS の認定とサードパーティによる証明	PCIDSSにおいてはWEPの利用を禁止している。			●	3	暗号化対策においては十分な強度を持った方式を利用する。加えて、構内LANにおいては、ネットワーク構成機器への未承認機器の論理的・物理的な接続を不可能とする、検疫ネットワークを導入する方法がある。	○	–	–	–	–	–	–	–	–	–	–	–	–	–
A43700001	技30	VI. 技術基準 II. 安全性検査対策	データ保護(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。	ファイル内容の矛盾発生防止のため、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。		適合可能	–	–	–	–	–			●	1	同一ファイルに複数のプログラムから同時更新がある場合は、データ内容に矛盾を起こし、結果的にファイル破壊となる。これを防止するため、ファイルに対する排他制御機能を設ける。	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A43800001	技31	VI. 技術基準 II. 安全性検査対策	データ保護(破壊・改ざん防止)	技31 ファイルに対するアクセス制御機能を設けること。	不正アクセス等からデータを保護するため、プログラムとファイル間のアクセス権限チェック機能等を設けること。	◎					適合可能	–	–	–	–	–			●	1	データを保護するため、重要なファイルについては、アクセス制御機能を設ける。具体的には、次の方法がある。 (1) OSの備えるアクセス制限の方法を使用 (2) DBMSの備えるアクセス制限の方法を使用 (3) アクセス制御専用のソフトウェアを使用	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A43900001	技32	VI. 技術基準 II. 安全性検査対策	データ保護(破壊・改ざん防止)	技32 不良データ検出機能を充実すること。	システムへの不良データの混入を防止するため、不良データの検出・除外機能を充実すること。	◎					適合可能	○	詳細版に記載	–	–	ISO 27001の管理策には、「通信及び運用管理」がある。			●	3	故意または過失により発生する不良データを検出する。具体的には、次の方法がある。 (1) 入力データのチェック (2) 処理履歴の確保	–	–	–	○	–	–	–	–	–	–	–	–	–

FISC 安全対策基準第8版および第8版追補からの引用									FISC安全対策基準に対するAWSの見解	FISC 安対基準への 適合性	クラウド事業者の対応 （Amazon Web Services）							SI事業者・利用者で必要な対応			クラウド特有の対応方法　○・・・対応必須、△・・・対応推奨																
																						クラウドの一般的対応方法				AWS特有の対応方法												
																						実装			プロセス		実装										プロセス
SEQ	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	必須とされている項目	第8版追補での改訂	追108関連			対応状況	開示レベル	実施内容 （参照された内容等）	公開文書への参照	第三者認証から類推出来る内容	AWS/ADSJへのインタビュー結果	NDAベース資料への参照	対応要否	対応パターン	対策例	暗号化	Antivirus	FW/IDS/IPS	キー・署名の外部管理	証跡等の保管場所	API	IAM	VPC	Multi-AZ	CloudWatch (EC2)	EBS/Snap Shot(EC2)	Auto Scaling (EC2)	ELB (EC2)	Management Cosole	Security Group	Direct Connect	AWSサポート
A44100001	技33	VI. 技術基準 II. 安全性検査対策	データ保護(検知策)	技33 伝送データの改ざん検知策を講ずること。	重要なデータの伝送において、改ざん検知のための対策を講じておくことが望ましい。	○			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 8.24に3.3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 SOC1タイプ2、SOC2タイプIIレポートに、AWSとの資産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。	適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type IIの認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要／コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス／AWS の認定とサードパーティによる証明				●	1	データ伝送において、重要なデータについては、改ざん検知のための対策を講じる。具体的には、次の方法がある。 (1) メッシージ認証コード (2) 電子署名	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A44200001	技34	VI. 技術基準 II. 安全性検査対策	データ保護(検知策)	技34 ファイル突合機能を設けること。	故意または過失により起きたファイル間の不整合を早期に発見するため、元帳、検査表、ジャーナル等のファイル間の突合機能を設けること。	◎				適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type IIの認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要／コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス／AWS の認定とサードパーティによる証明				●	1	故意または過失により起きたファイル間の内容不整合、論理エラー等を早期に発見する。具体的には、次の方法がある。 (1) 元帳、検査表、ジャーナル等のファイル間の内容を突合、検証する機能を設ける。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A44500001	技35	VI. 技術基準 II. 安全性検査対策	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。	不正使用防止のため、業務内容や接続方法に応じ、接続相手先がある.もしくは正当な端末であることを確認すること。	◎	■		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およびアクセス管理(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	適合可能	○	公開情報	・AWS は、顧客が自身の ID を確認し、AWS アカウントに安全にアクセスできるよう様々な方法を提供しています。	・Amazon Web Services: セキュリティプロセスの概要 /Amazon アカウントセキュリティ機能			ISO 27001の管理策には、「アクセス制御」がある。	●	2	接続相手先の正当性を確認する。具体的には、次の方法がある。 (1) 広義のパスワード (2) 暗号利用 (3) バイオメトリクス (4) 所有物 (5) 電子証明書およびネットワーク認証	○	–	–	○	–	–	○	–	–	–	–	–	–	–	–
A44600001	技35-1	VI. 技術基準 II. 安全性検査対策	不正使用防止(予防策(アクセス権限確認))	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。	生体認証の導入と運用にあたっては、技術面の最新動向等に留意し、その特性を十分考慮し、必要な安全対策を検討すること。	◎				適合可能	○	詳細版に記載	–	–	–			●	1	生体認証の導入と運用にあたっては、次の特性に考慮する。 (1) 認証精度 (2) 代替措置手続き (3) 否認防止 (4) 不正認証(なりすまし)等防止 (5) テンプレート保護技術	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A44700001	技36	VI. 技術基準 II. 安全性検査対策	不正使用防止(予防策(アクセス権限確認))	技36 IDの不正使用防止機能を設けること。	不正アクセス防止のため、システムやデータ等へのアクセスに用いるIDの不正使用防止機能を設けること。	◎				適合可能	○	公開情報	・AWS Identity and Access Management (AWS IAM) により、顧客が複数のユーザーを作成し、AWS アカウント内でそのユーザーごとにアクセス許可を管理できます。	・Amazon Web Services: セキュリティプロセスの概要 /AWS Identity and Access Management (AWS IAM)			ISO 27001の管理策には、「アクセス制御」がある。	●	1	不正使用を防止するための機能を組み込む。具体的には、次の方法がある。 (1) ログオン中のタイムアウト (2) 使用されないIDの使用停止 (3) ユーザーにログオン履歴情報を提供する	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A44800001	技37	VI. 技術基準 II. 安全性検査対策	不正使用防止(予防策(アクセス権限確認))	技37 アクセス履歴を管理すること。	アクセス状況を管理するため、システムやデータへのアクセス履歴を取得し、監査証跡として必要期間保管するとともに定期的にチェックすること。	◎				適合可能	○	詳細版に記載	–	–			ISO 27001の管理策には、「通信及び運用管理」がある。	●	1	アクセス履歴を取得し監査証跡として保管する。具体的には、次の方法がある。 (1) ログインとログオン状況 (2) 不正なアクセス要求 (3) システムによって失効とされたID	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A45000001	技38	VI. 技術基準 II. 安全性検査対策	不正使用防止(予防策(利用範囲の制限))	技38 取引制限機能を設けること。	不正アクセスを防止するため、端末等取引に使用する機器・媒体の種類、設置場所、用途等により、取引内容の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。	適合可能	–	–	–	–				●	1	端末等取引に使用する機器・媒体の種類、設置場所、用途等により、取引や業務内容の制限機能を設ける。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A45100001	技39	VI. 技術基準 II. 安全性検査対策	不正使用防止(予防策(利用範囲の制限))	技39 事故時の取引禁止機能を設けること。	カード、通帳、印鑑等の盗難・紛失等の事故に対処するため、その口座に対する当該媒体による取引を禁止する機能を設けること。また、渉外端末の盗難・紛失等の事故に対処するため、端末ごとの取引禁止機能を設けること。	◎				適合可能	–	–	–	–				●	1	事故に対処するため、その口座に対する当該媒体による取引を禁止する機能を設ける。また、渉外端末の盗難・紛失等の事故に対処するため、端末ごとの取引禁止機能を設ける。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A45300001	技40	VI. 技術基準 II. 安全性検査対策	不正使用防止(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。	不正使用防止のため、カードの偽造防止のための技術的措置を講ずることが望ましい。	○			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。	対象外	対象外	対象外	–	–				対象外																	
A45400001	技41	VI. 技術基準 II. 安全性検査対策	不正使用防止(予防策(不正・偽造防止対策))	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。	電子的価値のコピー、二重使用等の不正行為に対処するため、データの保護機能を具備するか、あるいはその発生を検知できる仕組みを構築しておくことが望ましい。	○				対象外	対象外	対象外	–	–				対象外																	
A45500001	技42	VI. 技術基準 II. 安全性検査対策	不正使用防止(予防策(不正・偽造防止対策))	技42 電子化された暗号鍵を重複する機器、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。	暗号鍵が他人に知られることによる不正行為を防止するため、暗号鍵の保護機能を機器、媒体またはソフトウェアに具備すること。	◎				適合可能	○	詳細版に記載	–	–			ISO 27001の管理策には、「情報システムの取得、開発及び保守」がある。	●	3	電子化された共通鍵、秘密鍵を重複するICカード等の機器、媒体あるいはそれに含まれるソフトウェアには、共通鍵、秘密鍵を保護する機能を具備する。	–	–	–	○	–	–	–	–	–	–	–	–	–	–	–
A45600001	技42-1	VI. 技術基準 II. 安全性検査対策	不正使用防止(予防策(不正・偽造防止対策))	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。	業務目的以外の電子メールの送受信やホームページの閲覧等に対処するため、不正使用防止対策を講ずることが望ましい。	○				適合可能	–	–	–	–				●	1	業務目的以外の電子メールの送受信やホームページの閲覧等に対処する。具体的には、次の方法がある。 (1) 利用者を適切な範囲に限定 (2) メールフィルタリング等を導入 (3) コンテンツフィルタリング等を導入	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A45800001	技43	VI. 技術基準 II. 安全性検査対策	不正使用防止(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。	不正侵入を防止するため、重要なデータやプログラムを扱うシステムについては、外部ネットワーク(オープンネットワーク、リモートアクセス等)との接続部分に適切な不正侵入防止策を講ずること。	◎	■		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および手順を確立しました。AWS SOC1タイプ2、SOC2タイプII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	適合可能	○	公開情報	・Amazon EC2 は、完全なファイヤウォールソリューションを提供します。	・Amazon Web Services: セキュリティプロセスの概要/Amazon Elastic Compute Cloud (Amazon EC2) のセキュリティ			ISO 27001の管理策には、「通信及び運用管理」がある。	●	2	AWS Security Group、サーバーのホスト型ファイアウォールの設定等によるネットワークからの入口対策に加えて、ネットワーク監視などの出口対策を実施することで横的な拡散に対する対応策を実施する。	–	–	○	–	–	–	–	–	–	–	○	–	–	–	–
A45900001	技44	VI. 技術基準 II. 安全性検査対策	不正使用防止(外部ネットワークからのアクセス制限)	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。	不正アクセスによるコンピュータシステムへの侵入を防ぐため、外部からアクセス可能な通信経路、通信関連機器等は最小限とし、不必要な機器は接続しないこと。	◎				適合可能	○	公開情報	・トラフィックは、プロトコル、サービスポート、ソース IP アドレス（個別 IP またはクラスなしドメイン間ルーティング（CIDR）ブロック）によって制限される場合があります。	・Amazon Web Services: セキュリティプロセスの概要/Amazon Elastic Compute Cloud (Amazon EC2) のセキュリティ			ISO 27001の管理策には、「通信及び運用管理、アクセス制御」がある。	●	2	AWS Security Group、サーバーのホスト型ファイアウォールの設定で ポートの制限等を行う。また、サーバー上で不要なサービスを停止または削除する。	–	–	○	–	–	–	–	–	–	–	○	–	–	–	–
A46100001	技45	VI. 技術基準 II. 安全性検査対策	不正使用防止(検知策)	技45 不正アクセスの監視機能を設けること。	不正アクセスの失敗や不正アクセスを監視する機能を設けること。	◎			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す。 AWSシステムに向け、AWSでは、ISO 27001認証に準拠するうえで、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および手順を確立しました。AWS SOC 1タイプ2、SOC2タイプII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。	適合可能	○	公開情報	・AWSネットワークは、既存のネットワークセキュリティの問題に対する強固な保護機能を提供しており、お客様はさらに堅牢な保護を行なうことができます。	・Amazon Web Services: セキュリティプロセスの概要/ネットワークセキュリティ			ISO 27001の管理策には、「アクセス制御」がある。	●	3	必要に応じて、ホスト型のIPS/IDS設置、OSの認証処理の監査機能の適用する。	–	–	○	–	–	–	–	–	–	–	–	–	–	–	–
A46200001	技46	VI. 技術基準 II. 安全性検査対策	不正使用防止(検知策)	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。	不正取引による被害発生の防止等のため、異常な取引状況を早期に把握するための機能を検討し実施すること。	◎				適合可能	–	–	–	–				●	1	異常な取引状況を把握するための機能を設けること。 具体的には、次の方法がある。 (1) カードの異常取引 (2) マネーロンダリングの疑いのある取引	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A46300001	技47	VI. 技術基準 II. 安全性検査対策	不正使用防止(検知策)	技47 異例取引の監視機能を設けること。	不正アクセスを早期に発見するため、異例取引の監視機能を設けること。	◎			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	適合可能	–	–	–	–				●	1	役席カードを使用するとともに、その使用記録を確認させる機能を設ける。具体的には、次の方法がある。 (1) 逆元帳票による方法 (2) オンライン照会による方法 (3) モニター専用(指定)端末による方法	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A46500001	技48	VI. 技術基準 II. 安全性検査対策	不正使用防止(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。	不正アクセスを検知した場合に備えて、不正アクセスの拡大防止のための対応策、復旧手順を明確にしておくことが望ましい。不正アクセスを検知した場合、その被害の有無にかかわらず、不正アクセスの拡大防止策、復旧策を講ずること。また、不正アクセスの原因を分析後、再発防止策を講ずること。	◎			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 8.32に13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 SOC1タイプ2、SOC2タイプIIレポートに、AWSとの資産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	適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type IIの認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明			ISO 27001の管理策には、「通信及び運用管理」情報セキュリティインシデントの管理」がある。	●	2	予防・発見に関しては、従来と同様の実施内容であり、個別案件のシステムで実装するが、AWSでは次の方法がある。 (1) 即時停止は、ManagementConsoleから実施 (2) 復旧手順としては、当該サーバでEBSを構成 (3) 調査・回復はVPCで閉鎖環境を構築 (4) SecurityGroupで通信を制御	–	–	–	–	–	–	–	○	○	○	–	–	–	–
A46800001	技49	VI. 技術基準 II. 安全性検査対策	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。	開発、保守、運用時におけるコンピュータウイルス等不正プログラムによる被害を防ぐため、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II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。	適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type IIの認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明			ISO 27001の管理策には、「通信及び運用管理」がある。	●	2	コンピュータウイルスの侵入や、不正アクセスによるプログラムの改ざん・去防止する対策を講ずる。具体的には、次の方法がある。 (1) アンチウィルス製品の導入 (2) 構成管理製品の導入 (3) FireWall製品の導入	–	○	○	–	–	–	–	–	–	–	○	–	–	–	–
A47000001	技50	VI. 技術基準 II. 安全性検査対策	不正プログラム防止(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。	システムの信頼性を確保・維持するため、コンピュータウイルス等の不正プログラムの侵入や組込みの有無を検証する検知対策を講ずること。	◎				適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type IIの認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明			ISO 27001の管理策には、「通信及び運用管理」がある。	●	3	不正プログラムの検知策や、その他システムの正当性を検証する対策を講ずること。具体的には、次の方法がある。 (1) スパイウェア対策ソフトの導入 (2) アクセス履歴管理ツールの導入 (3) 資源管理・監視ツールの導入	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–
A47200001	技51	VI. 技術基準 II. 安全性検査対策	不正プログラム防止(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。	コンピュータウイルス等の不正プログラムによる被害を最小限にするため、発見時からシステム復旧までの対策を講ずること。	◎				適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type IIの認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明			ISO 27001の管理策には、「通信及び運用管理」がある。	●	2	感染システムの切り離しと復旧の手段として、AWSでは次の対応も実施する。 (1) ManagementConsoleによる停止 (2) EBS.SnapShotからの復旧	–	–	–	–	–	○	–	–	○	–	–	–	–	–	–

【説明文】
FISC安対基準について、第8版追補での改訂内容の主な論点に対し、クラウド事業者やSI事業者/利用者の対応が必要か、その説明を記載した。

No.	第8版追補からの引用			セキュリティリファレンス改訂箇所			
	項目	論点	改訂方針	クラウド事業者の対応	SI事業者/利用者の対応	説明	備考
1	【設64】【設71】【設109】 自家発電装置の設置	自家発電装置の稼働時を想定した考慮点について記載すべきでないか。	稼働時を想定した自家発電装置の能力確認、及び燃料等の確保を考慮点として追記することとした。	○ 改訂無	対象外		
2	【運1】【運3】 セキュリティ管理の責任の明確化	セキュリティ管理のための環境整備について、経営層の関与を明確にすべきではないか。	セキュリティ管理のための文書や体制の整備にあたっては、経営層の主体的な関与が重要と考え、その旨を追記することとした。	○ 改訂無	● 改訂有	SI事業者/利用者は、システム運用におけるセキュリティの管理方針や体制の整備を進める上で、全社的な方針や体制に重大な影響を与えるものがある場合については、経営層の指示、承認を得た上で実施することを追記した。	本項目は、運108における管理事項として、参照されている。
3	【運50】 運用管理方法を明確にすること	スマートデバイスを業務利用する場合の留意点の記載が必要ではないか。	業務利用に関わる管理上の考慮点を見直し、機器特有のセキュリティに関する考慮点について、参考として追記することとした。	対象外 改訂無	● 改訂有	対象外としていたが、SI事業者・利用者で必要な対応に該当するものとした。SI事業者/利用者は、システム運用で渉外端末にスマートデバイスを利用する場合、機器の特性等による考慮点を踏まえた上で作業を実施することを追記した。	スマートデバイス等向けのアプリケーション「AWS Console」等を利用し、システム運用に関する操作を行うことを想定している。
4	【運62】 重大障害・災害についての経営層への報告	重大な障害・災害に伴う経営層への報告内容を定める必要はないか。	障害・災害による影響については、速やかな対応に向け、想定される最大リスクなどを含め、経営層へ報告を適宜行う必要がある旨を追記することとした。	○ 改訂無	● 改訂有	SI事業者/利用者は、重大な障害、災害については、想定される最大リスク等を含め経営層に報告するフローを策定することを追記した。	
5	【運62】【運84】 災害時の通信手段	災害時の通信途絶等を考慮すべきではないか。	災害時優先通信を含めた、複数の連絡手段の確保、及びその訓練の必要性について、追記することとした。	○ 改訂無	● 改訂有	災害時優先通信を含めた複数の連絡手段の確保、訓練の必要性について「SI事業者/利用者の対応」に追記した。	
6	【運63】 復旧手順	障害時・災害時の復旧手順について、見直すべきではないか。	バックアップシステムへの切り替え時の社内システムへの影響確認、切り戻しについて考慮点を追記することとした。	○ 改訂無	● 改訂有	切替時の影響確認、切り戻しについて考慮する旨を「SI事業者/利用者の対応」に追記した。	
7	【運64】 災害の再発防止や未然防止に向けた取組み	障害については、表面的な原因のみでなく、根本原因を分析し対応すべきではないか。	障害については、根本原因について、システム要因だけでなく、人的要因等も含め原因分析を行い、対策を講ずる必要がある旨を追記することとした。	○ 改訂無	● 改訂有	障害の未然防止、再発防止に向けての実行策を講ずる（かつ客観的に評価する）旨を追記。また、人的要因等を含めた障害発生原因を調査する旨追記した。	
8	【運64】 災害の再発防止や未然防止に向けた取組み	再発防止や未然防止に向けた態勢整備が必要ではないか。	障害の未然防止に向け、社内及び社外の障害情報を収集・分析し対策を講ずること、またその施策の実効性について客観的に評価する事が望ましい旨を追記することとした。				

No.	第8版追補からの引用			セキュリティリファレンス改訂箇所			
	項目	論点	改訂方針	クラウド事業者の対応	SI事業者/利用者の対応	説明	備考
9	【運67】 重要なシステムの開発プロジェクトの検証体制の整備	重要なシステムの開発プロジェクトにおける、社内横断的な検証体制について記載してはどうか。	関連する部門の状況を把握することも重要と考え、組織の検証体制についても参考として追記することとした。	- 改訂無	● 改訂無		
10	【運69】 移行判定	本番への移行手順で考慮するものとして、移行判定について記載すべきではないか。	移行作業の実施に当たって移行判定を行う事を手順に追記することとした。	- 改訂無	● 改訂無		
11	【運88】 外部委託契約	安全対策に関する項目を盛り込んだ委託契約の締結について、考慮点を追記すべきではないか。	目標復旧時間の記載や、SLAどおりに委託業務を遂行できない場合の対応策を事前に考慮しておくことが望ましい旨を追記することとした。	○ 改訂無	● 改訂有	クラウド事業者との管理境界、責任分界点に関する取り決めに準じ、SI事業者/利用者にてクラウドサービスが利用できなった場合を想定し対応策を講ずる旨追記した。	本項目は、運108における管理事項として、参照されている。
12	【運90】 外部委託先の点検と報告	委託先の業務運営状況について、経営層が把握しておくことが必要ではないか。	委託先の業務運営状況について確認した結果と認識した問題点について、経営層に適切に報告を行う必要がある旨を追記することとした。	○ 改訂無	● 改訂有	SI事業者/利用者は、経営者が利用しているクラウドサービスを理解した上で、リスク・対策を把握・判断できるようシステム監査、モニタリングを実施する旨追記した。	本項目は、運108における管理事項として、参照されている。
13	【運103】 不正使用を防止すること	スマートデバイスを使った金融サービスの提供には、機器特有のリスクの認識が必要ではないか。	紛失・盗難のリスク、URLが全表示されないことにより接続先を誤るリスクを参考として追記することとした。	○ 改訂無	● 改訂無		
14	【運105-1】 顧客への注意喚起事項	インターネットバンキングによる不正送金被害が増加しており、対策が必要ではないか。	口座の不正使用防止に関して顧客に注意喚起すべき事項を見直すこととした。	○ 改訂無	● 改訂無		
15	【運108】 クラウドサービスを対象とした安全対策基準の対応付け（基準の新設）	平成23年に実施した「金融機関におけるクラウドコンピューティングの利用動向に関する研究会」による調査で明らかとなった課題・問題点等について、安全対策基準への反映が必要ではないか。	クラウドサービスの利用は外部委託の一形態であるという認識のもと、その課題・問題点等について、「安全対策基準の対象に関する基本的な考え方」を踏まえ、その管理の考えかtについて、対象となる基準項目の改訂要否を含め検討を行っていくこととした。				
16		クラウドサービスに関する安全対策基準への反映については、参照の利便性を考慮すると既存基準の項目を改定するものではなく、新たな基準項目を新設する方が望ましいのではないか。	参照の利便性等を考慮し、基準を新設することとした。その際、クラウドサービス固有の留意事項は当該新設基準に記載し、既存の基準項目で読み取れる事項は該当する基準項目を参照する形とした。				
17		新設基準に記載の内容と、そこからの参照基準のみを参照すれば良いという認識を持たれないよう、表現を工夫すべきではないか。	本新設基準で参照していない各基準項目についても、必要に応じて参照すべき旨を記載することとした。				

No.	第8版追補からの引用			セキュリティリファレンス改訂箇所			
	項目	論点	改訂方針	クラウド事業者の対応	SI事業者/利用者の対応	説明	備考
18	【技2】【技3】【技4】【技5】【技6】 ハードウェアの予備の機能確認	障害発生時に、予備を含めたシステム全体が機能することを確認すべき旨を記載すべきではないか。	コンピュータを構成する本体装置、周辺装置・通信系装置・回線・端末系装置等について、障害発生時に、予備を含めたシステム全体が有効に機能することを確認しておく必要がある旨を追記することとした。	○ 改訂無	- 改訂無	AWSを構成する各要素の冗長性は十分に検証されているため、本項目は満たされていると判断し、変更は加えないこととした。	
19	【技7】 IPv4アドレスとIPv6アドレスが共存する環境	IPv4アドレスとIPv6アドレスが共存する環境の注意点を記載すべきではないか。	IPv4アドレスとIPv6アドレスが共存する環境の注意点や、IPv6環境で見られるセキュリティ上の課題について、参考として追記することとした。	○ 改訂有	● 改訂有	IPv4、IPv6に対するAWSの対応、並びに利用者が行うべき内容を追記した。	
20	【技25】 バックアップサイト	バックアップサイト保有の必要性について、より踏み込んだ記載が必要ではないか。	資金決済等の重要なシステムについては、バックアップサイトを保有することが必要であるが、保有しない場合は、代替手段について経営層による承認を必要とする旨を追記することとした。	○ 改訂無	● 改訂無	バックアップサイトに関してはこれまでの記載で内容が含まれているため、変更は加えないこととした。	
21	【技29】 無線LANの利用	一部の暗号については、短時間で解読ができるなど、危殆化が進んでおり、記載の見直しが必要ではないか。	WEPを業務システムにおいて利用しないことと、改訂時点での望ましい暗号方式について追記することとした。	○ 改訂有	● 改訂有	PCI-DSS Requirements and Security Assessment Procedures（https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf）4.1.1項にWEPの使用禁止に関する記述有り。"Note: The use of WEP as a security control was prohibited as of 30 June 2010."	PCI-DSS Requirements and Security Assessment Procedures
22	【技35】 不正使用防止 （アクセス権限確認）	インターネットバンキングにより不正送金被害が増加しており、対策が必要ではないか。	固定式のID・パスワードのみに頼らない認証方法の導入について追記することとした。	○ 改訂無	● 改訂有	論点にはインターネットバンキングとあり、アプリケーション層の対策であるのでクラウド事業者の対応としては記載を変更する必要が無いとした。SI事業者/利用者の対応としては第8版追補の内容に合わせて対応策を追記した。	
23	【技43】 不正使用防止 （外部ネットワークからのアクセス制限）	標的型攻撃による被害事例が増加していることから、対策を明記すべきではないか。	標的型攻撃への対策が現状確立されていないことから、効果の期待できる対策を参考として追記することとした。	○ 改訂有	● 改訂有	追加された標的型攻撃に対する対応についてIPAの公開ドキュメントの内容をベースに記載した。	IPA『標的型サイバー攻撃の事例分析と対策レポート』

FISC 安全対策基準第8版からの引用							FISC安全対策基準に対するAWSの見解	FISC 安対基準への適合性	クラウド事業者の対応（Amazon Web Services）						SI事業者・利用者で必要な対応			クラウド特有の対応方法　〇･･･対応必須、△･･･対応推奨																			
																			クラウドの一般的対応方法					AWS特有の対応方法													
																			実装			プロセス		実装												プロセス	
SEQ	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	必須とされている項目			対応状況	開示レベル	実施内容（参照された内容等）	公開文章への参照	第三者認証から類推出来る内容	AWS/ADSJへのインタビュー結果	NDAベース資料への参照	対応要否	対応パターン	対策例	暗号化	Antivirus	FW/IDS/IPS	キー・署名の外部管理	証跡等の保管場所	API	IAM	VPC	Multi-AZ	CloudWatch（EC2）	EBS/SnapShot(EC2)	Auto Scaling（EC2）	ELB（EC2）	Management Cosole	Security Group	Direct Connect	AWSサポート
	運108-1	運用基準 クラウドサービスの利用		クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。	クラウドサービスの利用は外部委託に相当すると認識し、適切なリスク管理を行うこと。	◎										●	1	クラウド利用は、委託例で、適切なリスク管理を行う事で、安全・安定な運用を実現する。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	運108-2-(1)	運用基準 クラウドサービスの利用		クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。	クラウドサービスの利用は外部委託に相当すると認識し、適切なリスク管理を行うこと。 (1)クラウドサービスを利用する場合の目的や範囲等の明確化【運37】	◎										●	1	クラウド利用に際しては、事前に目的や範囲を明確にする。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A35200001	運87	V. 運用基準	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。	システムの開発や運用等で外部委託を行う場合は、事前に目的や範囲等を明確にすることが必要である。	◎	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。	適合可能	○	詳細版に記載	–	–				●	1	システムの開発や運用で外部委託を行う場合は、事前に目的や業務範囲、形式、期間、費用、リスクの管理方法、委託先の選定条件、外部委託に関する自社窓口と役割等を明確にすること。再委託先等となるクラウド事業者が選定条件を満たせるか確認する。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	運108-2-(2)	運用基準 クラウドサービスの利用		クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。	クラウドサービスの利用は外部委託に相当すると認識し、適切なリスク管理を行うこと。 (2)クラウド事業者の選定手続きの明確化【運87-1】	◎										●	1	SI事業者は、委託に際して、自己評定として提示できるよう必要ドキュメントを整える事が望ましい。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A35300001	運87-1	V. 運用基準	外部委託管理(外部委託に関する計画)	運87-1 外部委託先の選定手続きを明確にすること。	外部委託先の選定に際しては手続きを明確にし、委託業者を客観的に評価すること。委託業者の決定にあたっては、責任者の承認を得ること。	◎	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。	適合可能	○	詳細版に記載	–	–				●	1	委託業者を選定するにあたっては、選定手続きを明確にし、安定性(財務内容)や健全性、組織体制、信頼度および受託実績、技術レベル等について外部委託先を客観的に評価して、委託業者の決定する。再委託先等となるクラウド事業者が選定条件を満たせるか確認する。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	運108-2-(3)	運用基準 クラウドサービスの利用		クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。	クラウドサービスの利用は外部委託に相当すると認識し、適切なリスク管理を行うこと。 (3)委託する形式に関わらず、安全対策に関する項目を盛り込んだ契約の締結【運88】	◎										●	1	1　機密保護、安全な業務遂行等を実現する為、安全対策を考慮すること。 2　品質の保証管理のため、SLA（Service Level Agreement）を締結するなど、委託契約期間中の継続的な評価に配慮する事が望ましい。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A35400001	運88	V. 運用基準	外部委託管理(外部委託に関する計画)	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。	安全性確保のため、機密保護、安全遂行等に関する項目を盛込んだ委託契約を締結すること。	◎	外部委託先の管理については、AWS利用者の責任となります。	適合可能	○	詳細版に記載	–	–				●	1	外部委託した業務が安全に遂行されるために、機密保護や安全な業務の遂行等を契約として外部委託先と締結するとともに、その契約の遵守状況を定期的に確認する、再委託先等となるクラウド事業者の安全対策を確認の上、締結する。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	運108-2-(3)-①	運用基準 クラウドサービスの利用		クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。	クラウドサービスの利用は外部委託に相当すると認識し、適切なリスク管理を行うこと。 (3)委託する形式に関わらず、安全対策に関する項目を盛り込んだ契約の締結【運88】 ①セキュリティ管理方法及び体制【運1，運3】	◎										●	3	以下の委託先金融機関等のセキュリティ管理方針との整合を図ること。 (1)セキュリティポリシー (2)セキュリティスタンダード (3)マニュアルや手順書 なお、例外的な対策が必要な場合および管理方針では不明確な事項については、委託・受託の双方で協議のうえ進める。	△	△	△	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A21500001	運1	V. 運用基準	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。	セキュリティ管理を適切に行うため、セキュリティ管理の具体的手順、責任等を明確にし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よって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	適合可能	○	公開情報	・ISO 27001の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001管理策「情報セキュリティのための組織」,「通信及び運用管理／運用の手順及び責任」に従った対策の実施。			●	1	セキュリティ管理の具体的手、責任等を明確にした文書を整備すること。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A21700001	運3	V. 運用基準	管理体制の確立(セキュリティ管理と責任の明確化)	運3　セキュリティ管理体制を整備すること。	セキュリティ管理を適切に行うため、セキュリティ管理の責任者等を定め、その職務範囲と権限および責任について定めること。	◎		適合可能	○	公開情報	・ISO 27001の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001管理策「情報セキュリティのための組織」,「通信及び運用管理／運用の手順及び責任」に従った対策の実施。			●	1	セキュリティ管理方針と手順に従ってシステムが運用されていることを管理するためのセキュリティ管理体制（組織、職務範囲、権限等）を整備する。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	運108-2-(3)-②	運用基準 クラウドサービスの利用		クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。	クラウドサービスの利用は外部委託に相当すると認識し、適切なリスク管理を行うこと。 (3)委託する形式に関わらず、安全対策に関する項目を盛り込んだ契約の締結【運88】 ②システム管理体制、データ管理体制、ネットワーク管理体制【運4～6】	◎										●	1	安全かつ円滑な運用と不正防止のため、システム管理体制、データ管理体制、ネットワーク管理体制を明確化すること。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A21800001	運4	V. 運用基準	管理体制の確立(セキュリティ管理と責任の明確化)	運4　システム管理体制を整備すること。	システムの安全かつ円滑な運用と不正防止のため、システムの管理手順を定め、管理体制を整備すること。	◎	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よって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	適合可能	○	公開情報	・ISO 27001の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001管理策「情報セキュリティのための組織」,「通信及び運用管理／運用の手順及び責任」に従った対策の実施。			●	1	管理対象となる仮想マシン（ゲストOS）及びその上で稼働するソフトウェアについて、システム管理手順を定め、それらの手順を実現する管理体制を整備する。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A21900001	運5	V. 運用基準	管理体制の確立(セキュリティ管理と責任の明確化)	運5　データ管理体制を整備すること。	データの安全かつ円滑な運用と不正防止のため、データ管理手順を定め、管理体制を整備すること。	◎		適合可能	○	公開情報	・ISO 27001の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001管理策「情報セキュリティのための組織」,「通信及び運用管理／運用の手順及び責任」に従った対策の実施。			●	1	管理対象となるデータを明確にした上で、そのデータ管理手順を定め、管理体制を整備する。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A22000001	運6	V. 運用基準	管理体制の確立(セキュリティ管理と責任の明確化)	運6　ネットワーク管理体制を整備すること。	コンピュータネットワークの適切かつ効率的な運用と不正アクセス等の防止のため、ネットワークの管理手順を定め、管理体制を整備すること。	◎		適合可能	○	公開情報	・ISO 27001の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	ISO 27001管理策「情報セキュリティのための組織」,「通信及び運用管理／運用の手順及び責任」に従った対策の実施。			●	1	システム運用環境からAWS環境に接続する箇所を含め、自社システム側のネットワークの管理手順および利用承認手続き等を管理手順として定め、関係者に周知徹底させることにより、ネットワークの適切かつ効率的で安全な運用を行う。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	運108-2-(3)-③	運用基準 クラウドサービスの利用		クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。	クラウドサービスの利用は外部委託に相当すると認識し、適切なリスク管理を行うこと。 ③委託する形式に関わらず、安全対策に関する項目を盛り込んだ契約の締結【運88】 ③障害時・災害時のマニュアル整備、復旧手順、及び教育・訓練【運15，運83，運85】	◎										●	1	障害・災害時の影響の最小化と早期復旧について、受託元金融機関等と整合のとれた対策とする。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A23700001	運15	V. 運用基準	運用管理(マニュアルの整備)	運15　障害時・災害時マニュアルを整備すること。	障害・災害によるコンピュータシステムへの影響の極小化と早期復旧ならびに本部・営業店等における業務継続のため、障害時・災害時における代替措置、復旧手順および対応方法等について定めた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て、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に照り定義され、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タイプレポートで確認する事が出来ます。	適合可能	○	公開情報	・ISO 27001を始め、SOC1 Type II、SOC2 Type II、PCI DSS Level 1の認証を取得している。	・Amazon Web Services: セキュリティプロセスの概要/コントロール環境の概略 ・Amazon Web Services: リスクとコンプライアンス/AWS の認定とサードパーティによる証明	・SOC1　Control Objective8: Incident Handlingの基準に従った対策を実施。 ・ISO 27001管理策「情報セキュリティインシデントの管理」に従った対策の実施。			●	1	障害時・災害時における代替措置、復旧手順および対応方法等について定めたマニュアルを整備する。そのマニュアルは定期的に見直しを行う。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
A31100001	運63	V. 運用基準	運用管理(障害時・災害時対応策)	運63　障害時・災害時復旧手順を明確にすること。	障害または災害等によりコンピュータシステムが正常に稼働しなくなった場合の復旧手順を明確にすること。なお、当該手順については、コンティンジェンシープランと整合性のとれた内容にすること。	◎	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。 http://aws.amazon.com/security	適合可能	○	公開情報	・Amazon の内部監査グループは、最近になって 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。	・Amazon Web Services: セキュリティプロセスの概要/事業継続性管理				●	2	障害時・災害時復旧手順とは、障害または災害等により正常に稼働しなくなったコンピュータシステムを復旧させるための手続きを明確にしたものである。AWSでは、複数のアベイラビリティゾーンを利用した復旧も考慮する。	–	–	–	–	–	–	–	○	–	–	–	–	–	–	–	–	–	–
A34400001	運83	V. 運用基準	教育・訓練(教育・訓練)	運83　障害時・災害時に備えた教育・訓練を行うこと。	障害時・災害時に備えるため、コンピュータシステムの運用に係わるオペレーション等の教育・訓練を行うこと。	◎	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。 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	適合可能	○	公開情報	・当社は構造化された実行プロセスに従い、新入社員がAmazon のツール、プロセス、システム、ポリシーおよび手順を熟知できるよう教育を行っています。	・Amazon Web Services: リスクとコンプライアンス/ AWS リスクおよびコンプライアンスプログラム	教育を定期的に実施。			●	1	通常のシステム運用と同様に、 障害時・災害時におけるコンピュータシステムの運用を円滑に行うため、障害時・災害時マニュアルおよびコンティンジェンシープランに基づいたオペレーションの教育・訓練を定期的に行う。また、訓練結果については、責任者を明確にし、分析・評価のうえ、次回訓練およびコンティンジェンシープランに反映する。	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	運108-2-(3)-④	運用基準 クラウドサービスの利用		クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。	クラウドサービスの利用は外部委託に相当すると認識し、適切なリスク管理を行うこと。 (3)委託する形式に関わらず、安全対策に関する項目を盛り込んだ契約の締結【運88】 ④クラウドサービスを利用するためのデータバックアップ【運27】	◎											2	委託元金融機関等のセキュリティ管理方針に沿い、重要な業務等については、ファイルの障害や災害等の対応のため、バックアップを取得し、その管理方法を明確化しておくこと。	–	–	–	–	–	△	–	–	–	○	–	–	–	–	–	–	–	–
A25300001	運27	V. 運用基準	運用管理(データファイル管理)	運27　バックアップを確保すること。	重要なデータファイルの障害や災害等への対応のため、バックアップを取得し、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、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。	適合可能	–	–	–	–	–	–	●	2	AWS上に格納された重要なデータファイルやAmazon マシンイメージ（AMI）のバックアップを取得し、管理方法を明確にする。バックアップデータの種別により、バックアップ先を自社システムのストレージにするか、AWS上のAmazon S3等のストレージにするか検討する。	–	–	–	–	○	△	○	–	△	–	○	–	–	–	–	–	–

FISC 安全対策基準第8版からの引用							FISC安全対策基準に対するAWSの見解	FISC 安対基準への適合性	クラウド事業者の対応（Amazon Web Services）						SI事業者・利用者で必要な対応			クラウド特有の対応方法　〇・・・対応必須、△・・・対応推奨																
																		クラウドの一般的対応方法					AWS特有の対応方法												
																		実装		プロセス			実装											プロセス	
SEQ	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	必須とされている項目			対応状況	開示レベル	実施内容（参照された内容等）	公開文章への参照	第三者認証から類推出来る内容	AWS/ADSJへのインタビュー結果	NDAベース資料への参照	対応要否	対応パターン	対策例	暗号化	Antivirus	FW/IDS/IPS	キー・署名の外部管理	証跡等の保管場所	API	IAM	VPC	Multi-AZ	CloudWatch (EC2)	EBS/SnapShot(EC2)	Auto Scaling (EC2)	ELB (EC2)	Management Cosole	Security Group	Direct Connect	AWSサポート
	運108-2-(3)-⑤	運用基準 クラウドサービスの利用		クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。	クラウドサービスの利用は外部委託に相当すると認識し、適切なリスク管理を行うこと。 ③委託する形式に関わらず、安全対策に関する項目を盛り込んだ契約の締結【運88】 ⑤クラウドサービスの利用を中止または終了する場合のデータ消去【運75】	◎											●	1	管理項目を定め、クラウド事業者での対応可否を明確にする。対応ができない場合は、リスク回避の為の手段を講じる。またリスク管理項目の妥当性を定期的に見直しを行い、必要に応じて改善する。	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
A33000001	運75	V.　運用基準	システム開発・変更（システムの廃棄）	運75　情報漏洩防止対策を講ずること。	機密保護や不正防止等のため、システムの廃棄にあたっては機器等から情報漏洩が生じないように防止策を講ずること。	◎	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。	適合可能	○	公開情報	・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。	・Amazon Web Services: セキュリティプロセスの概要／ストレージデバイスの廃棄				●	3	内部の重要なデータを読み出し不可能とするために、利用者側としては、蓄積データを暗号化することでサービス提供側のディスク廃棄時の情報漏洩対策を施すことができる。	○	－	－	○	○	－	－	－	－	－	－	－	－	－	－	－
	運108-2-(4)	運用基準 クラウドサービスの利用		クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。	クラウドサービスの利用は外部委託に相当すると認識し、適切なリスク管理を行うこと。 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り決めが他国である場合のリスク評価。	◎											●	1	管理項目を定め、クラウド事業者での対応可否を明確にする。対応ができない場合は、リスク回避の為の手段を講じる。またリスク管理項目の妥当性を定期的に見直しを行い、必要に応じて改善する。 クラウド事業者との係争を加味し、利用者が対応可能な取決めを行う事。	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
	運108-2-(4)-①	運用基準 クラウドサービスの利用		クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。	クラウドサービスの利用は外部委託に相当すると認識し、適切なリスク管理を行うこと。 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り決めが他国である場合のリスク評価。 ①現地の各種法制や裁判制度の把握と分析	◎											●	1	管理項目を定め、クラウド事業者での対応可否を明確にする。対応ができない場合は、リスク回避の為の手段を講じる。またリスク管理項目の妥当性を定期的に見直しを行い、必要に応じて改善する。 クラウド事業者との係争を加味し、利用者が対応可能な取決めを行う事。	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
	運108-2-(4)-②	運用基準 クラウドサービスの利用		クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。	クラウドサービスの利用は外部委託に相当すると認識し、適切なリスク管理を行うこと。 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り決めが他国である場合のリスク評価。 ②現地での活動資格を有する弁護士の確保	◎											●	1	管理項目を定め、クラウド事業者での対応可否を明確にする。対応ができない場合は、リスク回避の為の手段を講じる。またリスク管理項目の妥当性を定期的に見直しを行い、必要に応じて改善する。 クラウド事業者との係争を加味し、利用者が対応可能な取決めを行う事。	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
	運108-2-(4)-③	運用基準 クラウドサービスの利用		クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。	クラウドサービスの利用は外部委託に相当すると認識し、適切なリスク管理を行うこと。 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り決めが他国である場合のリスク評価。 ③地理不案内な遠隔地での打ち合わせや出廷などに伴う経済的、人的負担	◎											●	1	管理項目を定め、クラウド事業者での対応可否を明確にする。対応ができない場合は、リスク回避の為の手段を講じる。またリスク管理項目の妥当性を定期的に見直しを行い、必要に応じて改善する。 クラウド事業者との係争を加味し、利用者が対応可能な取決めを行う事。	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
	運108-2-(4)-④	運用基準 クラウドサービスの利用		クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。	クラウドサービスの利用は外部委託に相当すると認識し、適切なリスク管理を行うこと。 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り決めが他国である場合のリスク評価。 ④上記全てについての外国語での対応	◎											●	1	管理項目を定め、クラウド事業者での対応可否を明確にする。対応ができない場合は、リスク回避の為の手段を講じる。またリスク管理項目の妥当性を定期的に見直しを行い、必要に応じて改善する。 クラウド事業者との係争を加味し、利用者が対応可能な取決めを行う事。	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
	運108-3	運用基準 クラウドサービスの利用		クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。	クラウドサービスの利用は外部委託に相当すると認識し、適切なリスク管理を行うこと。 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、遵守正、及び安全性の面から把握、評価するため、システム監査を実施することが必要である。 システム監査については【運90、運91】を参照	◎											●	1	管理項目を定め、クラウド事業者での対応可否を明確にする。対応ができない場合は、リスク回避の為の手段を講じる。またリスク管理項目の妥当性を定期的に見直しを行い、必要に応じて改善する。 有効性、効率性、信頼性、遵守性、安全面に関する基準を設け、監査により基準を満たしているか確認できるようにする。また必要であれば、システム運用にて統計情報を蓄積する事で、基準到達状況を確認できるようにする。	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
A35700001	運90	V.　運用基準	外部委託管理（外部委託業務管理）	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。	外部に委託した業務内容を確認するため、業務組織の整備を行うとともに、委託契約に基づき管理、検証を行うこと。	◎		適合可能	○	詳細版に記載	–	–				●	1	金融機関等が外部委託した業務が安全に運行されるために、機密保護や安全な業務の遂行等を契約として外部委託先と締結するとともに、その契約の遵守状況を定期的に確認する。再委託先等となるクラウド事業者の管理状況を確認する。	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
A36100001	運91	V.　運用基準	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。	コンピュータシステムおよびその管理について、有効性、効率性、信頼性、遵守性、および安全性の面から把握、評価するため、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。	適合可能	○	詳細版に記載	–	–				●	2	通常のシステム運用と同様に、 コンピュータシステムの運用、システム開発・変更等においては、コンピュータシステムの有効性、効率性、信頼性、遵守性、および安全性を確保するため、コンピュータ部門から独立したシステム監査人がシステムの総合的な監査・評価を行い、経営層に監査結果を報告する。 また、委託先経由でAWSプレミアムサポート(エンタープライズ)への監査内容の確認や内部監査部門による監査内容の確認を行う。	－	－	－	－	○	－	－	－	－	－	－	－	－	－	－	△
	運108-4	運用基準 クラウドサービスの利用		クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。	クラウドサービスの利用は外部委託に相当すると認識し、適切なリスク管理を行うこと。 本基準項目で参照していない、設備基準や技術基準、及び外部委託管理以外の運用基準についても、必要に応じて参照すること。	◎											●	1	管理項目を定め、クラウド事業者での対応可否を明確にする。対応ができない場合は、リスク回避の為の手段を講じる。またリスク管理項目の妥当性を定期的に見直しを行い、必要に応じて改善する。 利用者にて必要な運用基準を適宜参照する。	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
	運108-5	運用基準 クラウドサービスの利用		クラウドサービスの利用にあたっては、適切なリスク管理を行うこと。	クラウドサービスの利用は外部委託に相当すると認識し、適切なリスク管理を行うこと。 参照している各基準に「委託契約」という文言がある場合は、「利用契約」や「利用規約」等の「サービスを利用するための契約」に読み替えて参照のこと。	◎											●	1	管理項目を定め、クラウド事業者での対応可否を明確にする。対応ができない場合は、リスク回避の為の手段を講じる。またリスク管理項目の妥当性を定期的に見直しを行い、必要に応じて改善する。 参照している各基準に「委託契約」という文言がある場合は、「利用契約」や「利用規約」等の「サービスを利用するための契約」に読み替えて参照する。	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－