部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
2	情報セキュリティ対策の基本的枠組み					対象外			
3	情報の取扱い								
3	3.1	情報の取扱い							
3	3.1	3.1.1	情報の取扱い						
3	3.1	3.1.1	(1)		情報の取扱いに係る規定の整備				
3	3.1	3.1.1	(1)	(a)	統括情報セキュリティ責任者は、以下を含む情報の取扱いに関する規定を整備し、職員等へ周知すること。	対象外			
3	3.1	3.1.1	(1)	(a)	(ア) 情報の格付及び取扱制限についての定義	対象外			
3	3.1	3.1.1	(1)	(a)	(イ) 情報の格付及び取扱制限の明示等についての手続	対象外			
3	3.1	3.1.1	(1)	(a)	(ウ) 情報の格付及び取扱制限の継承、見直しに関する手続	対象外			
3	3.1	3.1.1	(2)		情報の目的外での利用等の禁止				
3	3.1	3.1.1	(2)	(a)	職員等は、自らが担当している業務の遂行のために必要な範囲に限って、情報を利用等すること。	対象外			
3	3.1	3.1.1	(3)		情報の格付及び取扱制限の決定・明示等				
3	3.1	3.1.1	(3)	(a)	職員等は、情報の作成時及び機関等外の者が作成した情報を入手したことに伴う管理の開始時に、格付及び取扱制限の定義に基づき格付及び取扱制限を決定し、明示等すること。	対象外			
3	3.1	3.1.1	(3)	(b)	職員等は、情報を作成又は複製する際に、参照した情報又は入手した情報に既に格付及び取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付及び取扱制限を継承すること。	対象外			
3	3.1	3.1.1	(3)	(c)	職員等は、修正、追加、削除その他の理由により、情報の格付及び取扱制限を見直す必要があると考える場合には、情報の格付及び取扱制限の決定者（決定を引き継いだ者を含む。）又は決定者の上司（以下本款において「決定者等」という。）に確認し、その結果に基づき見直すこと。	対象外			
3	3.1	3.1.1	(4)		情報の利用・保存				
3	3.1	3.1.1	(4)	(a)	職員等は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱うこと。	対象外	利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱うことは、クラウドサービス利用有無にかかわらず、職員等が遵守すべき事項である。	利用する情報に明示された格付及び取扱制限に従い、当該情報を適切に取り扱うことについては、本リファレンスの説明の対象外。	
3	3.1	3.1.1	(4)	(b)	職員等は、機密性３情報について要管理対策区域外で情報処理を行う場合は、情報システムセキュリティ責任者及び課室情報セキュリティ責任者の許可を得ること。	対象外	機密性３情報について要管理対策区域外で情報処理を行う場合に情報システムセキュリティ責任者及び課室情報セキュリティ責任者の許可を得ることは、クラウドサービス利用有無にかかわらず、職員等が遵守すべき事項である。	機密性３情報について要管理対策区域外で情報処理を行う場合に情報システムセキュリティ責任者及び課室情報セキュリティ責任者の許可を得ることについては、本リファレンスの説明の対象外。	
3	3.1	3.1.1	(4)	(c)	職員等は、要保護情報について要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講ずること。	対象外	要保護情報について要管理対策区域外で情報処理を行う場合に必要な安全管理措置を講ずることは、クラウドサービス利用有無にかかわらず、職員等が遵守すべき事項である。	要保護情報について要管理対策区域外で情報処理を行う場合に必要な安全管理措置を講ずることについては、本リファレンスの説明の対象外。	
3	3.1	3.1.1	(4)	(d)	職員等は、保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること。	適合可能	・職員等は、情報を保存する場合には、AWSクラウドを利用する場合も、AWSクラウドの利用の無い従来の情報システムと同様に情報の格付及び取扱制限に従って情報を適切に管理する必要がある。 [留意事項] ・AWSは信頼性、拡張性、安全性に優れたストレージサービス、データベースサービスを提供しており、利用者はこれらのサービスを利用し情報を保存することが可能であるかを評価し、最適な情報の保存方法を検討することが望ましい。 ・AWSクラウドのサービスを利用して情報を保存する場合は、各サービスで管理可能な内容や対象範囲を確認し、適切なオプション選択や設定をする必要があることに留意する。 ・AWSクラウドのサービスを活用して情報を保存する場合は、情報を保存するリージョンを適切に選択する必要があることに留意する。	・AWSが提供するストレージサービス、データベースサービスは、アクセスコントロール、暗号化、アクセスログなどの機能を提供しており、利用者はこれらの機能を利用し情報を適切に保管することが可能である。 ・AWSクラウドは、データとサーバーを配置する物理的なリージョンを利用者が指定することができ、原則、AWSが利用者コンテンツを移動しないため、利用者は情報を保存する場所に日本を指定することが可能である。	クラウドストレージはクラウドコンピューティングに不可欠のコンポーネントで、アプリケーションが使用する情報を保持します。ビッグデータ分析、データウェアハウス、モノのインターネット、データベース、バックアップとアーカイブのすべてのアプリケーションが、何らかの形態のデータストレージアーキテクチャに依存します。クラウドストレージは、通常、従来のオンプレミスストレージシステムよりも信頼性、拡張性、安全性に優れています。 詳細に関してはhttps://aws.amazon.com/jp/products/storage/?nc2=h_l3_dbを参照してください。 AWS のフルマネージドデータベースサービスには、トランザクショナルアプリケーション用のリレーショナルデータベース、インターネットスケールアプリケーション用の非リレーショナルデータベース、分析用データウェアハウス、キャッシュとリアルタイムワークロード用のインメモリデータストア、高度に接続されたデータを扱うアプリケーション構築用のグラフデータベースがあります。既存のデータベースの AWS への移行をご検討の場合は、AWS Database Migration Service を活用いただくことで、簡単に、高い費用対効果で移行することができます。 詳細に関してはhttps://aws.amazon.com/jp/products/databases/?nc2=h_l3_dbを参照してください。 セキュリティは、AWS のインフラストラクチャのすべての層だけではなく、そのインフラストラクチャで利用できるすべてのサービスにも組み込まれています。AWS サービスのアーキテクチャは、すべての AWS ネットワークおよびプラットフォームと効率的かつ安全に連動するように設計されています。各サービスに豊富なセキュリティ機能が用意されており、これらを活用して機密データおよびアプリケーションを保護できます。 詳細に関しては「セキュリティプロセスの概要 （2014年11月版）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf データとサーバーを配置する物理的なリージョンは、AWS のお客様が指定します。S3 データオブジェクトのデータレプリケーションは、データが保存されているリージョンのクラスタ内で実行され、他のリージョンの他のデータセンタークラスタにはレプリケートされません。データとサーバーを配置する物理的なリージョンは、AWS のお客様が指定します。AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しないものとします。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS のお客様は、お客様のデータの統制と所有権を保持します。AWS はお客様のプライバシー保護を慎重に考慮し、AWS が準拠する必要がある法的処置の要求についても注意深く判断しています。AWS は、法的処置による命令に確実な根拠がないと判断した場合は、その命令にためらわずに異議を申し立てます。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf
					なお、独立行政法人及び指定法人における職員等は、機密性３情報を機器等に保存する際、以下の措置を講ずること。	対象外			
3	3.1	3.1.1	(4)	(d)	(ア) 機器等に保存する場合は、インターネットや、インターネットに接点を有する情報システムに接続しない端末、サーバ装置等の機器等を使用すること。	対象外	機密性３情報を機器等に保存する場合において、インターネットや、インターネットに接点を有する情報システムに接続しない端末、サーバ装置等の機器等を使用することは、クラウドサービス利用有無にかかわらず、独立行政法人及び指定法人における職員等が遵守すべき事項である。	機密性３情報を機器等に保存する場合において、インターネットや、インターネットに接点を有する情報システムに接続しない端末、サーバ装置等の機器等を使用することについては、本リファレンスの説明の対象外。	

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
3	3.1	3.1.1	(4)	(d)	(イ) 当該情報に対し、暗号化による保護を行うこと。	対象外	当該情報に対し、暗号化による保護を行うことは、クラウドサービス利用有無にかかわらず、独立行政法人及び指定法人における職員等が遵守すべき事項である。	当該情報に対し、暗号化による保護を行うことについては、本リファレンスの説明の対象外。	
3	3.1	3.1.1	(4)	(d)	(ウ) 当該情報を保存した機器等について、盗難及び不正な持ち出し等の物理的な脅威から保護するための対策を講ずること。	対象外	当該情報を保存した機器等について、盗難及び不正な持ち出し等の物理的な脅威から保護するための対策を講ずることは、クラウドサービス利用有無にかかわらず、独立行政法人及び指定法人における職員等が遵守すべき事項である。	当該情報を保存した機器等について、盗難及び不正な持ち出し等の物理的な脅威から保護するための対策を講ずることについては、本リファレンスの説明の対象外。	
3	3.1	3.1.1	(4)	(e)	職員等は、USB メモリ等の外部電磁的記録媒体を用いて情報を取り扱う際、定められた利用手順に従うこと。	対象外	USBメモリ等の外部電磁的記録媒体を用いて情報を取り扱う際に定められた利用手順に従うことは、クラウドサービス利用有無にかかわらず、職員等が遵守すべき事項である。	USBメモリ等の外部電磁的記録媒体を用いて情報を取り扱う際に定められた利用手順に従うことについては、本リファレンスの説明の対象外。	
3	3.1	3.1.1	(5)	情報の提供・公表					
3	3.1	3.1.1	(5)	(a)	職員等は、情報を公表する場合には、当該情報が機密性１情報に格付されるものであることを確認すること。	対象外			
3	3.1	3.1.1	(5)	(b)	職員等は、閲覧制限の範囲外の者に情報を提供する必要が生じた場合は、当該格付及び取扱制限の決定者等に相談し、その決定に従うこと。また、提供先において、当該情報に付された格付及び取扱制限に応じて適切に取り扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講ずること。	対象外			
3	3.1	3.1.1	(5)	(c)	独立行政法人及び指定法人における職員等は、機密性３情報を閲覧制限の範囲外の者に提供する場合には、課室情報セキュリティ責任者の許可を得ること。	対象外			
3	3.1	3.1.1	(5)	(d)	職員等は、電磁的記録を提供又は公表する場合には、当該電磁的記録等からの不用意な情報漏えいを防止するための措置を講ずること。	対象外			
3	3.1	3.1.1	(6)	情報の運搬・送信					
3	3.1	3.1.1	(6)	(a)	職員等は、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、安全確保に留意して運搬方法を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。独立行政法人及び指定法人における職員等が、機密性３情報を要管理対策区域外に持ち出す場合には、暗号化措置を施した上で、課室情報セキュリティ責任者が指定する方法により運搬すること。ただし、他機関等の要管理対策区域であって、統括情報セキュリティ責任者があらかじめ定めた区域のみに持ち出す場合は、当該区域を要管理対策区域とみなすことができる。	適合可能	・職員等は、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、AWSクラウドを利用する場合も、AWSクラウドを利用しない従来の情報システムと同様に、安全確保に留意して運搬方法を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずる必要がある。 [留意事項] ・AWSが取得しているISO 27001、ISO 27017、ISO 27018、ISO 9001基準、および PCI DSS 認証を確認の上、AWSクラウド利用が適切であるかを判断する必要があることに留意する。 ・AWSクラウドを利用して業務を実施する区域等ユーザー側で管理すべき区域から情報を持ち出す場合は、従来どおり安全確保のための適切な措置を講ずる必要があることに留意する。 ・暗号化機能については、AWSクラウドの暗号化機能のほか、情報システム独自に暗号化機能を実装することも選択肢となることに留意する。	・AWSクラウドは、データとサーバーを配置する物理的なリージョンを利用者が指定することができ、原則、AWSが利用者コンテンツを移動しないため、利用者は情報を保存する場所を指定することが可能である。 ・AWSのセキュリティフレームワークは、NIST 800-53、ISO 27001、ISO 27017、ISO 27018、ISO 9001 基準、および PCI DSSに準拠し、ポリシーと手続きを規程しており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSクラウドは、データの暗号化機能を提供しており、当該機能を用いることで、機密性３情報に対し、暗号化措置を施すことが可能である。	データとサーバーを配置する物理的なリージョンは、AWS のお客様が指定します。S3 データオブジェクトのデータレプリケーションは、データが保存されているリージョンのクラスタ内で実行され、他のリージョンの他のデータセンタークラスタにはレプリケートされません。データとサーバーを配置する物理的なリージョンは、AWS のお客様が指定します。AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しないものとします。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS のお客様は、お客様のデータの統制と所有権を保持します。AWS はお客様のプライバシー保護を慎重に考慮し、AWS が準拠する必要がある法的処置の要求についても注意深く判断しています。AWS は、法的処置による命令に確実な根拠がないと判断した場合は、その命令にためらわずに異議を申し立てます。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS セキュリティフレームワークは、NIST 800-53、ISO 27001、ISO 27017、ISO 27018、ISO 9001 基準、および PCI DSS 要件に基づいて、ポリシーと手続きを規定しています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS は、情報および関連技術のための統制目標 (COBIT) フレームワークに基づいて情報セキュリティフレームワークとポリシーを制定していて、ISO 27002 統制、米国公認会計士協会 (AICPA) の信頼提供の原則 (Trust Services Principles)、PCI DSS 3.1 版、および米国国立標準技術研究所 (NIST) 出版物 800-53 改訂 3 (連邦情報システム向けの推奨セキュリティ管理) に基づいて ISO 27001 認定可能なフレームワークを実質的に統合しています。AWS は、ISO 27001 基準に合わせてサードパーティーとの関係を管理しています。AWS サードパーティーの要件は、PCI DSS、ISO 27001、および FedRAMP への準拠のため、監査中に外部の独立監査人によって確認されます。AWS コンプライアンスプログラムに関する情報は、http://aws.amazon.com/compliance/ のウェブサイトに一般公開されています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS は、従業員にセキュリティポリシーおよびセキュリティトレーニングを提供することで、情報セキュリティに関する役割と責任について教育しています。Amazon の基準またはプロトコルに違反した従業員は調査され、適切な懲戒 (警告、業績計画、停職、解雇など) が実施されます。 詳細については、次のウェブサイトで入手可能な AWS クラウドセキュリティホワイトペーパーを参照してください。http://aws.amazon.com/security。詳細については、ISO 27001 基準の付録 A、ドメイン 7 を参照してください。AWS は、 ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWSにはスケーラブルで効果的な暗号化機能が提供されており、クラウド内に保管中のデータのセキュリティをより一層強化できます。これには以下が含まれます。 ☆EBS、S3、Glacier、Oracle RDS、SQL Server RDS、およびRedshiftといった、AWSのストレージおよびデータベースサービスに利用できる、データの暗号化機能 ☆暗号化キーをAWS側で管理するか、完全に自分で管理するかを選択できる、AWS Key Management Serviceなどの柔軟なキー管理オプション ☆コンプライアンスの要件を満たすことを可能にする、AWS CloudHSMを使用した専用の、ハードウェアベースの暗号化キーストレージ さらに、AWSには、AWS環境内でお客様が開発またはデプロイされたどのサービスにも暗号化とデータ保護を統合できるAPIが用意されています。詳細に関しては、 https://aws.amazon.com/jp/security/を参照してください。 AWS は、AWS インフラストラクチャ内で採用される必要な暗号化用の暗号キーを内部的に確立、管理しています。AWS は NIST で承認されたキー管理テクノロジーとプロセスを AWS 情報システムで使用して対称暗号キーを作成、管理、配布しています。対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストで必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認証をセキュリティ保護、配布するために使用されます。AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001 、および FedRAMP への AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
3	3.1	3.1.1	(6)	(b)	職員等は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。独立行政法人及び指定法人における職員等が、機密性３情報を機関等外通信回線（インターネットを除く。）を使用して送信する場合には、暗号化措置を施した上で、課室情報セキュリティ責任者が指定する方法により送信すること。	対象外	要保護情報である電磁的記録を電子メール等で送信する場合、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずることは、クラウドサービス利用有無にかかわらず、職員等が遵守すべき事項である。	要保護情報である電磁的記録を電子メール等で送信する場合、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずることについては、本リファレンスの説明の対象外。	
3	3.1	3.1.1	(7)	情報の消去					
3	3.1	3.1.1	(7)	(a)	職員等は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去すること。	対象外	電磁的記録媒体に保存された情報が職務上不要となった場合、速やかに情報を消去することは、クラウドサービス利用有無にかかわらず、職員等が遵守すべき事項である。	電磁的記録媒体に保存された情報が職務上不要となった場合、速やかに情報を消去することについては、本リファレンスの説明の対象外。	
3	3.1	3.1.1	(7)	(b)	職員等は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消すること。	適合可能	・職員等は、電磁的記録媒体を廃棄する場合には、AWSクラウドを利用する場合も、AWSクラウドを利用しない従来の情報システムと同様に、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消すること。 [留意事項] ・AWSクラウド上のデータ管理に関しては、提供される暗号化機能やサービスを利用した暗号化を実施し、システム利用終了時に暗号鍵そのものを廃棄することで、データ抹消に相当するといった対応を考慮することも可能である。	・AWSクラウドは、ストレージデバイスが製品寿命に達した場合、DoD 5220.22-M（「国家産業セキュリティプログラム運営マニュアル」）やNIST 800-88（「媒体のサニタイズに関するガイドライン」）の基準に準拠し廃棄を行っており、利用者は、これらの認証を取得していることを確認可能である。 ・削除した EBS ボリュームが使用していた物理的なブロックストレージは、別のアカウントに割り当てられる前に、ゼロで上書きされる。	AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M (国家産業セキュリティプログラム運営マニュアル) または NIST 800-88 (媒体のサニタイズに関するガイドライン) に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。詳細については、次のウェブサイトで入手可能な AWS クラウドセキュリティホワイトペーパーを参照してください。 http://aws.amazon.com/security/。 Amazon EBS ボリュームは、ワイプ処理を行った後、未フォーマットのロープロックデバイスとしてお客様に提供されます。ワイプは再使用の直前に実施されるため、お客様に提供された時点でワイプ処理は完了しています。業務手順上、DoD 5220.22-M（「国家産業セキュリティプログラム運営マニュアル」）や NIST 800-88（「媒体のサニタイズに関するガイドライン」）が指定するような、特定の方法で全データをワイプする必要がある場合、お客様自身で Amazon EBS のワイプ作業を行うこともできます。お客様がしかるべき手順でワイプを実施してからボリュームを削除することで、コンプライアンスの要件を満たすようにします。 機密データの暗号化は、一般的なセキュリティのベストプラクティスです。AWS には、EBS ボリュームとスナップショットを AES-256 で暗号化する機能があります。EC2 インスタンスをホストするサーバーで暗号化が行われるため、EC2 インスタンスと EBS ストレージとの間を移動するデータが暗号化されます。この処理が効率的に低レイテンシーで行われるようにするために、EBS 暗号化機能は EC2 の強力なインスタンスタイプ (たとえば、M3、C3、R3、G2) だけで使用できます。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf ISO 27001 基準に合わせて、AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M (国家産業セキュリティプログラム運営マニュアル) または NIST 800-88 (媒体のサニタイズに関するガイドライン) に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。 詳細については、ISO 27001 基準の付録 A、ドメイン 8 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf データの永続性 データは、ボリュームを明示的に削除するまでボリュームに保持されます。削除した EBS ボリュームが使用していた物理的なブロックストレージは、別のアカウントに割り当てられる前に、ゼロで上書きされます。機密データを扱っている場合は、手動によるデータの暗号化や、Amazon EBS 暗号化 で保護されているボリュームへのデータの格納を検討してください。詳細については、「Amazon EBS Encryption」を参照してください。 デフォルトでは、インスタンスの起動時に作成およびアタッチされた EBS ボリュームは、インスタンスの終了時に削除されます。この動作を変更するには、インスタンスの起動時にフラグ DeleteOnTermination の値を false に変更します。値を変更すると、インスタンスが終了してもボリュームが保持されるので、そのボリュームを別のインスタンスにアタッチできます。 詳細に関しては、http://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSVolumes.html を参照してください。
3	3.1	3.1.1	(7)	(c)	職員等は、要機密情報である書面を廃棄する場合には、復元が困難な状態にすること。	対象外	要機密情報である書面を廃棄する場合、復元が困難な状態にすることは、クラウドサービス利用有無にかかわらず、職員等が遵守すべき事項である。	要機密情報である書面を廃棄する場合、復元が困難な状態にすることについては、本リファレンスの説明の対象外。	
3	3.1	3.1.1	(8)	情報のバックアップ					

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
3	3.1	3.1.1	(8)	(a)	職員等は、情報の格付に応じて、適切な方法で情報のバックアップを実施すること。	適合可能	職員等は、情報の格付に応じて、適切な方法で情報のバックアップを実施すること。	・AWSのストレージサービスは、アクセスコントロール、暗号化、アクセスログなどの機能を提供しており、利用者はこれらの機能を活用し、適切な方法で情報のバックアップを行うことが可能である。 ・利用者は、AWSのデータコンプライアンスについて、SOCレポートにて独立監査法人によって保証されていることを確認可能である。 ・AWSクラウドは、データとサーバーを配置する物理的なリージョンを利用者が指定することができ、原則、AWSが利用者コンテンツを移動しないため、利用者は情報のバックアップを保管する国を日本に指定することが可能である。 ・Amazon S3 と Amazon Glacier の設計上の耐久性は 99.999999999%であり、利用者は高い耐久性を持つストレージに情報のバックアップを保管することが可能である。 ・Amazon マシンイメージ (AMI) は、サーバ（インスタンス）イメージをバックアップすることができる機能であり、サーバ（インスタンス）が運用できなくなった場合に正常な運用状態に復元することが可能である。 ・AWSは、利用者が自身のデータの統制と所有権を保持しており、AWSストレージからデータを出力し利用者が別途用意した環境にデータバックアップを保管することが可能である。	アマゾン ウェブ サービスが提供するストレージソリューションは、オンプレミス環境に物理的なインフラを構築することなく、バックアップと復旧環境を実現します。また、オンプレミスとクラウドの相互運用による移行も可能です。柔軟で拡張性の高い IT リソースをクラウドに準備し、耐久性と拡張性に優れたストレージをご利用いただけます。 ・SOC1 などの AWS セキュリティ認定が、データのコンプライアンスを確実にします。保存データの暗号化を可能にする AES 256 などの標準によって、データを守ります。Amazon Virtual Private Cloud を使えば、データベースとアプリケーションサーバ用の社内向けサブネットを作成し、ミッションクリティカルなワークロードへのセキュリティコントロールを強化できます。 ・AWS のストレージソリューションなら、レイテンシーの最適化、コストの最小化、または法規制要件への対処を目的として、データをどのリージョンに保管するかを選択できます。データはお客様が完全にコントロールできます。11 のリージョンと幅広いアベイラビリティーゾーンがあり、保護を強化するために指定された複数の AZ にデータが分散されるので、データの保存場所に関しては柔軟性を持たせることができます。 ・Amazon S3 と Amazon Glacier では、データセンター間でデータが自動的にレプリケートされ、設計上の耐久性は 99.999999999% となっています。AWS のストレージソリューションは堅牢なデータ保護を提供するので、データの保存場所を心配する必要はありません。 詳細に関してはhttps://aws.amazon.com/jp/backup-recovery/をご参照下さい。 データとサーバーを配置する物理的なリージョンは、AWS のお客様が指定します。S3 データオブジェクトのデータレプリケーションは、データが保存されているリージョンのクラスタ内で実行され、他のリージョンの他のデータセンタークラスタにはレプリケートされません。データとサーバーを配置する物理的なリージョンは、AWS のお客様が指定します。AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しないものとします。 詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf 'お客様は、お客様のデータの統制と所有権を保持します。お客様は、AMI をエクスポートして、施設内または別のプロバイダーで使用できます (ただし、ソフトウェアのライセンス制限に従います)。詳細については、AWS セキュリティプロセスの概要ホワイトペーパー (http://aws.amazon.com/security) を参照してください。 AWS では、必要に応じてお客様がデータを AWS ストレージから出し入れすることを許可しています。S3 用 AWS Import/Export サービスでは、転送用のポータブル記憶装置を使用して、AWS 内外への大容量データの転送を高速化できます。AWS では、お客様がご自分のテープバックアップサービスプロバイダーを使用してテープへのバックアップを実行することを許可しています。ただし、AWS ではテープへのバックアップサービスを提供していません。 AWS データセンターは、世界のさまざまなリージョンにクラスター化されて構築されています。すべてのデータセンターはオンラインで顧客にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、影響を受けたエリアから顧客データが移動されます。重要なアプリケーションは N+1 原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。AWS は、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。各アベイラビリティーゾーンは、独立した障害ゾーンとして設計されています。つまり、アベイラビリティーゾーンは、一般的な都市地域内で物理的に分離されており、洪水の影響が及ばないような場所にあります (洪水地域の分類はリージョンによって異なります)。個別の無停電電源装置 (UPS) やオンサイトのバックアップ生成施設に加え、シングルポイントの障害の可能性を減らすために、別々の電力供給施設から異なる配管網を経由して、個別に電力供給を行っています。これらはすべて、冗長的に、複数の Tier-1 プロバイダーに接続されています。顧客は AWS の使用量を計画しながら、複数のリージョンやアベイラビリティーゾーンを利用する必要があります。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配信することによって、自然災害やシステム障害など、ほとんどの障害モードに対して、その可用性を保つことができます。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
3	3.1	3.1.1	(8)	(b)	職員等は、取得した情報のバックアップについて、格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理すること。	適合可能	・職員等は、AWSクラウドを利用する場合も、AWSクラウドを利用しない従来の情報システムと同様に、取得した情報のバックアップについて、格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理する必要がある。 [留意事項] ・AWSが取得しているISO27001の認証やSOCレポートを確認の上、ユーザがAWSクラウドに情報のバックアップを保存するかを判断する。 ・AWSクラウドのサービスを活用して情報のバックアップを取得する場合は、各サービスで提供する機能及び制約事項を確認し、AWSクラウドのサービスでは要件を満たせない場合には、バックアップツールや改ざん防止ツールなどの導入、外部媒体でのデータ保管などの検討(設計、導入、運用）する必要があることに留意する。	・AWSクラウドは、データとサーバーを配置する物理的なリージョンを利用者が指定することができ、原則、AWSが利用者コンテンツを移動しないため、利用者は情報のバックアップを保管する国を日本に指定することが可能である。 ・利用者は、AWSのデータコンプライアンスについて、SOCレポートにて独立監査法人によって保証されていることを確認可能である。 ・Amazon S3 と Amazon Glacier の設計上の耐久性は 99.999999999%であり、利用者は高い耐久性を持つストレージに情報のバックアップを保管することが可能である。 ・AWSのデータセンターは、ISO27001認証に基づき環境リスクへの物理的な保護を行っており、利用者は災害に強く、高い可用性を備えたデータセンターに情報のバックアップを保管することが可能である。	アマゾン ウェブ サービスが提供するストレージソリューションは、オンプレミス環境に物理的なインフラを構築することなく、バックアップと復旧環境を実現します。また、オンプレミスとクラウドの相互運用による移行も可能です。柔軟で拡張性の高い IT リソースをクラウドに準備し、耐久性と拡張性に優れたストレージをご利用いただけます。 ・SOC1 などの AWS セキュリティ認定が、データのコンプライアンスを確実にします。保存データの暗号化を可能にする AES 256 などの標準によって、データを守ります。Amazon Virtual Private Cloud を使えば、データベースとアプリケーションサーバ用の社内向けサブネットを作成し、ミッションクリティカルなワークロードへのセキュリティコントロールを強化できます。 ・AWS のストレージソリューションなら、レイテンシーの最適化、コストの最小化、または法規制要件への対処を目的として、データをどのリージョンに保管するかを選択できます。データはお客様が完全にコントロールできます。11 のリージョンと幅広いアベイラビリティーゾーンがあり、保護を強化するために指定された複数の AZ にデータが分散されるので、データの保存場所に関しては柔軟性を持たせることができます。 ・Amazon S3 と Amazon Glacier では、データセンター間でデータが自動的にレプリケートされ、設計上の耐久性は 99.999999999% となっています。AWS のストレージソリューションは堅牢なデータ保護を提供するので、データの保存場所を心配する必要はありません。 詳細に関してはhttps://aws.amazon.com/jp/backup-recovery/をご参照下さい。 AWS のお客様は、お客様のデータの統制と所有権を保持します。AWS は、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。各アベイラビリティーゾーンは、独立した障害ゾーンとして設計されています。障害時には、自動プロセスが、顧客データを影響を受けるエリアから移動します。AWS SOC 1 Type 2 レポートに詳細情報が記載されています。ISO 27001 基準の付録 A、ドメイン 11.2 に詳細が記載されています。AWS は独立監査人により ISO 27001 認定に準拠している旨の審査と認定を受けています。お客様は、AWS を利用すると、予備の物理データセンターのインフラストラクチャ費用を発生させることなく、重要な IT システムの迅速な復旧が可能になります。AWS クラウドでは、一般的な災害復旧 (DR) アーキテクチャの多くがサポートされています。たとえば、「パイロットライト」環境では瞬時にスケールアップが可能であり、「ホットスタンバイ」環境では高速フェイルオーバーが可能です。AWS の災害復旧の詳細については、https://aws.amazon.com/disaster-recovery/ を参照してください。 AWS は、堅牢な継続性計画を実装する機能をお客様に提供しています。たとえば、頻繁なサーバーインスタンスバックアップの利用、データの冗長レプリケーション、マルチリージョン/アベイラビリティーゾーンのデプロイアーキテクチャなどです。AWS は、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。各アベイラビリティーゾーンは、独立した障害ゾーンとして設計されています。障害時には、自動プロセスが、顧客データを影響を受けるエリアから移動します。 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組み込んでいます。環境リスクに対する AWS の物理的な保護は、独立監査人によって検証され、ISO 27002 のベストプラクティスに準拠していると認定されました。詳細については、ISO 27001 基準の付録 A、ドメイン 9.1 および AWS SOC 1 Type II レポートを参照してください。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS のお客様は、お客様のコンテンツの統制と所有権を有していますので、データのバックアッププランを管理するのはお客様の責任です。 AWS では、必要に応じてお客様がデータを AWS ストレージから出し入れすることを許可しています。S3 用 AWS Import/Export サービスでは、転送用のポータブル記憶装置を使用して、AWS 内外への大容量データの転送を高速化できます。AWS では、お客様がご自分のテープバックアップサービスプロバイダーを使用してテープへのバックアップを実行することを許可しています。ただし、AWS ではテープへのバックアップサービスを提供していません。Amazon S3 サービスはデータ損失の可能性をほぼ 0% にまで低減する設計になっており、データストレージの冗長化によってデータオブジェクトのマルチサイトコピーに匹敵する永続性を実現しています。データの永続性と冗長性については、AWS のウェブサイトをご覧ください。 AWS は、災害復旧をサポートするためにさまざまなクラウドコンピューティングサービスを提供しています。AWS の災害復旧の詳細については、 https://aws.amazon.com/disaster-recovery/ を参照してください。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf
3	3.1	3.1.1	(8)	(c)	職員等は、保存期間を過ぎた情報のバックアップについては、前条の規定に従い、適切な方法で消去、抹消又は廃棄すること。	適合可能	・職員等は、保存期間を過ぎた情報のバックアップについては、AWSクラウドを利用する場合も、AWSクラウドを利用しない従来の情報システムと同様に、本項(7)の規定に従い、適切な方法で消去、抹消又は廃棄する必要がある。 [留意事項] ・AWSクラウド上のデータ管理に関しては、提供される暗号化機能やサービスを利用した暗号化を実施し、システム利用終了時に暗号鍵そのものを廃棄することで、データ抹消に相当するといった対応を考慮することも可能である。	・AWSクラウドは、ストレージデバイスが製品寿命に達した場合、ISO27001の基準に準拠し廃棄を行っており、利用者は、これらの認証を取得していることを確認可能である。 ・削除した EBS ボリュームが使用していた物理的なブロックストレージは、別のアカウントに割り当てられる前に、ゼロで上書きされる。	AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M (国家産業セキュリティプログラム運営マニュアル) または NIST 800-88 (媒体のサニタイズに関するガイドライン) に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。詳細については、次のウェブサイトで入手可能な AWS クラウドセキュリティホワイトペーパーを参照してください。 http://aws.amazon.com/security/。 Amazon EBS ボリュームは、ワイプ処理を行った後、未フォーマットのローブロックデバイスとしてお客様に提供されます。ワイプは再使用の直前に実施されるため、お客様に提供された時点でワイプ処理は完了しています。業務手順上、DoD 5220.22-M (「国家産業セキュリティプログラム運営マニュアル」) や NIST 800-88 (「媒体のサニタイズに関するガイドライン」) が指定するような、特定の方法で全データをワイプする必要がある場合、お客様自身で Amazon EBS のワイプ作業を行うこともできます。お客様がしかるべき手順でワイプを実施してからボリュームを削除することで、コンプライアンスの要件を満たすようにします。 機密データの暗号化は、一般的なセキュリティのベストプラクティスです。AWS には、EBS ボリュームとスナップショットを AES-256 で暗号化する機能があります。EC2 インスタンスをホストするサーバーで暗号化が行われるため、EC2 インスタンスと EBS ストレージとの間を移動するデータが暗号化されます。この処理が効率的に低レイテンシーで行われるようにするために、EBS 暗号化機能は EC2 の強力なインスタンスタイプ (たとえば、M3、C3、R3、G2) だけで使用できます。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf ISO 27001 基準に合わせて、AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M (国家産業セキュリティプログラム運営マニュアル) または NIST 800-88 (媒体のサニタイズに関するガイドライン) に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。 詳細については、ISO 27001 基準の付録 A、ドメイン 8 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf データの永続性 データは、ボリュームを明示的に削除するまでボリュームに保持されます。削除した EBS ボリュームが使用していた物理的なブロックストレージは、別のアカウントに割り当てられる前に、ゼロで上書きされます。機密データを扱っている場合は、手動によるデータの暗号化や、Amazon EBS 暗号化 で保護されているボリュームへのデータの格納を検討してください。詳細については、「Amazon EBS Encryption」を参照してください。 デフォルトでは、インスタンスの起動時に作成およびアタッチされた EBS ボリュームは、インスタンスの終了時に削除されます。この動作を変更するには、インスタンスの起動時にフラグ DeleteOnTermination の値を false に変更します。値を変更すると、インスタンスが終了してもボリュームが保持されるので、そのボリュームを別のインスタンスにアタッチできます。 詳細に関しては、http://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSVolumes.html を参照してください。
3	3.2	情報を取り扱う区域の管理							
3	3.2	3.2.1	情報を取り扱う区域の管理						
3	3.2	3.2.1	(1)	要管理対策区域における対策の基準の決定					

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
3	3.2	3.2.1	(1)	(a)	統括情報セキュリティ責任者は、要管理対策区域の範囲を定めること。	対象外	要管理対策区域の範囲を定めることは、クラウドサービス有無にかかわらず、統括情報セキュリティ責任者が検討すべき事項である。	要管理対策区域の範囲を定めることについては、本リファレンスの説明の対象外。	
3	3.2	3.2.1	(1)	(b)	統括情報セキュリティ責任者は、要管理対策区域の特性に応じて、以下の観点を含む対策の基準を定めること。	対象外	要管理対策区域の特性に応じて対策の基準を定めることについては、情報システム利用有無にかかわらず、統括情報セキュリティ責任者が検討すべき事項である。	要管理対策区域の特性に応じて対策の基準を定めることについては、本リファレンスの説明の対象外。	
3	3.2	3.2.1	(1)	(b)	(ア) 許可されていない者が容易に立ち入ることができないようにするための、施錠可能な扉、間仕切り等の施設の整備、設備の設置等の物理的な対策。	適合可能	・統括情報セキュリティ責任者は、要管理区域の対策基準を定めるにあたり、AWSクラウドを利用する場合も、AWSクラウドを利用しない従来の情報システムと同様に、許可されていない者が容易に立ち入ることができないようにするための、施錠可能な扉、間仕切り等の施設の整備、設備の設置等の物理的な対策基準を定める必要がある。 [留意事項] ・AWSが取得しているISO27001等の認証やSOCレポートで、AWSの物理的セキュリティ対策を確認の上、AWSクラウド利用が可能であるか判断する。 ・AWSクラウドを利用して業務を実施する区域などユーザー側で管理すべき区域においては、当該区域のセキュリティ対策を定め利用することに留意する。	・AWSはPCI DSS,ISO27001に準拠して許可されていない者が容易に立ち入ることができないようにするための物理的な対策を実施しており、利用者は、これらの認証を取得していることを確認可能である。 ・利用者は、AWSの物理的セキュリティメカニズムについて、SOCレポートにて独立監査人によって保証されていることを確認可能である。	Amazon のデータセンターは最新式で、革新的で建築的かつ工学的アプローチを採用しています。Amazon は大規模データセンターの設計、構築、運用において、長年の経験を有しています。この経験は、AWS プラットフォームとインフラストラクチャに活かされています。AWS のデータセンターは、外部からはそれとはわからないようになっています。ビデオ監視カメラ、最新鋭の侵入検出システム、その他エレクトロニクスを使った手段を用いて、専門のセキュリティスタッフが、建物の入口とその周辺両方において、物理的アクセスを厳密に管理しています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行います。AWS は、そのような権限に対して正規のビジネスニーズがある従業員や業者に対してのみデータセンターへのアクセ スや情報を提供しています。従業員がこれらの特権を必要とする作業を完了したら、たとえかれらが引き続き Amazonまたは Amazon Web Services の従業員であったとしても、そのアクセス権は速やかに取り消されます。AWS 従業員によるデータセンターへのすべての物理的アクセスは記録され、定期的に監査されます。 詳細に関しては「セキュリティプロセスの概要 （2014年11月版）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf 物理的セキュリティ統制には、フェンス、壁、保安スタッフ、監視カメラ、侵入検知システム、その他の電子的手段などの境界統制が含まれますが、それに限定されるものではありません。AWS SOC レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。詳細については、ISO 27001 基準の付録 A、ドメイン 11 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf 物理的アクセスは、建物の周辺および入り口において、監視カメラや侵入検知システムなどの電子的手段を用いる専門の保安要員その他の手段により、厳重に管理されています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。サーバー設置箇所への物理アクセスポイントは、AWS データセンター物理セキュリティポリシーの規定により、閉回路テレビ (CCTV) カメラで録画されています。 AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO 27001、および FedRAMP への準拠のため、監査中に外部の独立監査人によって確認されます。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf
3	3.2	3.2.1	(1)	(b)	(イ) 許可されていない者の立入りを制限するため及び立入りを許可された者による立入り時の不正な行為を防止するための入退管理対策。	適合可能	・統括情報セキュリティ責任者は、要管理区域の対策基準を定めるにあたり、AWSクラウドを利用する場合も、AWSクラウドを利用する場合も、AWSクラウドを利用しない従来の情報システムと同様に、許可されていない者の立入りを制限するため及び立入りを許可された者による立入り時の不正な行為を防止するための入退管理対策を検討する必要がある。 [留意事項] ・AWSが取得しているISO27001等の認証やSOCレポートで、AWSの物理的セキュリティ対策を確認の上、AWSクラウド利用が可能であるか判断する。 ・AWSクラウドを利用して業務を実施する区域などユーザー側で管理すべき区域においては、当該区域のセキュリティ対策を定め利用することに留意する。	・AWSはPCI DSS,ISO27001に準拠して許可されていない者の立入の制限と許可された者による立ち入り時の不正行為を防止するための入退館管理を実施しており、利用者は、これらの認証を取得していることを確認可能である。 ・利用者は、AWSの物理的セキュリティメカニズムについて、SOCレポートにて独立監査人によって保証されていることを確認可能である。	Amazon のデータセンターは最新式で、革新的で建築的かつ工学的アプローチを採用しています。Amazon は大規模データセンターの設計、構築、運用において、長年の経験を有しています。この経験は、AWS プラットフォームとインフラストラクチャに活かされています。AWS のデータセンターは、外部からはそれとはわからないようになっています。ビデオ監視カメラ、最新鋭の侵入検出システム、その他エレクトロニクスを使った手段を用いて、専門のセキュリティスタッフが、建物の入口とその周辺両方において、物理的アクセスを厳密に管理しています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行います。AWS は、そのような権限に対して正規のビジネスニーズがある従業員や業者に対してのみデータセンターへのアクセ スや情報を提供しています。従業員がこれらの特権を必要とする作業を完了したら、たとえかれらが引き続き Amazonまたは Amazon Web Services の従業員であったとしても、そのアクセス権は速やかに取り消されます。AWS 従業員によるデータセンターへのすべての物理的アクセスは記録され、定期的に監査されます。 詳細に関しては「セキュリティプロセスの概要 （2014年11月版）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf 物理的セキュリティ統制には、フェンス、壁、保安スタッフ、監視カメラ、侵入検知システム、その他の電子的手段などの境界統制が含まれますが、それに限定されるものではありません。AWS SOC レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。詳細については、ISO 27001 基準の付録 A、ドメイン 11 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf 物理的アクセスは、建物の周辺および入り口において、監視カメラや侵入検知システムなどの電子的手段を用いる専門の保安要員その他の手段により、厳重に管理されています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。サーバー設置箇所への物理アクセスポイントは、AWS データセンター物理セキュリティポリシーの規定により、閉回路テレビ (CCTV) カメラで録画されています。 AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO 27001、および FedRAMP への準拠のため、監査中に外部の独立監査人によって確認されます。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf
3	3.2	3.2.1	(2)	区域ごとの対策の決定					
3	3.2	3.2.1	(2)	(a)	情報セキュリティ責任者は、統括情報セキュリティ責任者が定めた対策の基準を踏まえ、施設及び執務環境に係る対策を行う単位ごとの区域を定めること。	対象外			
3	3.2	3.2.1	(2)	(b)	区域情報セキュリティ責任者は、管理する区域について、統括情報セキュリティ責任者が定めた対策の基準と、周辺環境や当該区域で行う業務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定すること。	対象外			
3	3.2	3.2.1	(3)	要管理対策区域における対策の実施					

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
3	3.2	3.2.1	(3)	(a)	区域情報セキュリティ責任者は、管理する区域に対して定めた対策を実施すること。職員等が実施すべき対策については、職員等が認識できる措置を講ずること。	適合可能	・区域情報セキュリティ責任者は、AWSクラウドを利用する場合も、AWSクラウドを利用しない従来の情報システムと同様に、管理する区域に対して定めた対策を実施する必要がある。 [留意事項] ・AWSが取得しているISO27001等の認証やSOCレポートで、AWSのセキュリティ統制を確認の上、AWSクラウド利用が可能であるか判断する。 ・AWSクラウドを利用して業務を実施する区域などユーザー側で管理すべき区域においては、当該区域のセキュリティ対策を定め利用することに留意する。	・AWSはISO27001などの認定に準拠し、情報セキュリティフレームワーク、ポリシーを制定しており、利用者は、これらの認証を取得していることを確認可能である。 ・利用者は、AWSのセキュリティ統制について、SOCレポートにて独立監査人によって保証されていることを確認可能である。	AWS は、外部の認定機関および独立監査人と連携し、コンプライアンスフレームワークへの準拠を確認および検証しています。AWS SOC レポートには、AWS が実行している具体的な物理的セキュリティ統制活動に関する詳細情報が記載されています。詳細については、ISO 27001 基準の付録 A、ドメイン 11 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf Amazon の統制環境は、当社の最上層部で開始されます。役員とシニアリーダーは、当社のカラーと中心的な価値を規定する際、重要な役割を担っています。各従業員には当社の業務行動倫理規定が配布され、定期的なトレーニングを受けます。作成したポリシーを従業員が理解し、従うために、コンプライアンス監査が実施されます。詳細については、AWS リスクとコンプライアンスホワイトペーパー (http://aws.amazon.com/compliance) を参照してください。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS はお客様に ISO 27001 認定を提供しています。ISO 27001 認定は特に AWS ISMS に焦点を合わせており、AWS の内部プロセスがどのように ISO 基準に従っているかを測定します。認定とは、サードパーティーによる承認を受けた独立監査機関が AWS のプロセスおよびコントロールを評価し、ISO 27001 認定基準に沿って運用されていることを検証したことを意味します。詳細については、AWS Compliance ISO 27001 FAQ ウェブサイトを参照してください。 http://aws.amazon.com/compliance/iso-27001-faqs/。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS セキュリティフレームワークは、NIST 800-53、ISO 27001、ISO 27017、ISO 27018、ISO 9001 基準、および PCI DSS 要件に基づいて、ポリシーと手続きを規定しています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS は、情報および関連技術のための統制目標 (COBIT) フレームワークに基づいて情報セキュリティフレームワークとポリシーを制定していて、ISO 27002 統制、米国公認会計士協会 (AICPA) の信頼提供の原則 (Trust Services Principles)、PCI DSS 3.1 版、および米国国立標準技術研究所 (NIST) 出版物 800-53 改訂 3 (連邦情報システム向けの推奨セキュリティ管理) に基づいて ISO 27001 認定可能なフレームワークを実質的に統合しています。AWS は、ISO 27001 基準に合わせてサードパーティーとの関係を管理しています。AWS サードパーティーの要件は、PCI DSS、ISO 27001、および FedRAMP への準拠のため、監査中に外部の独立監査人によって確認されます。AWS コンプライアンスプログラムに関する情報は、http://aws.amazon.com/compliance/ のウェブサイトに一般公開されています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS は、従業員にセキュリティポリシーおよびセキュリティトレーニングを提供することで、情報セキュリティに関する役割と責任について教育しています。 Amazon の基準またはプロトコルに違反した従業員は調査され、適切な懲戒 (警告、業績計画、停職、解雇など) が実施されます。 詳細については、次のウェブサイトで入手可能な AWS クラウドセキュリティホワイトペーパーを参照してください。http://aws.amazon.com/security。詳細については、ISO 27001 基準の付録 A、ドメイン 7 を参照してください。AWS は、 ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf
3	3.2	3.2.1	(3)	(b)	区域情報セキュリティ責任者は、災害から要安定情報を取り扱う情報システムを保護するために物理的な対策を講ずること。	適合可能	・区域情報セキュリティ責任者は、AWSクラウドを利用する場合も、AWSクラウドを利用しない従来の情報システムと同様に、災害から要安定情報を取り扱う情報システムを保護するために物理的な対策を講ずる必要がある。 [留意事項] ・AWSが取得しているISO27001等の認証やSOCレポートで、AWSの環境リスクに対する物理的な対策内容を確認の上、AWSクラウド利用が可能であるか判断する。 ・AWSクラウドを利用して業務を実施する区域などユーザー側で管理すべき区域においては、火災などの環境リスクに対し当該区域の物理的対策を講ずる必要があることに留意する。	・AWSクラウドのデータセンターは、ISO 27001認定に基づき、災害などの環境リスクに対する物理的な対策を施しており、利用者はこれらの認証を取得していることを確認可能である。 ・利用者は、AWSの物理的セキュリティ統制活動について、SOCレポートにて独立監査人によって保証されていることを確認可能である。	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組み込んでいます。環境リスクに対する AWS の物理的な保護は、独立監査人によって検証され、 ISO 27002 のベストプラクティスに準拠していると認定されました。 詳細については、ISO 27001 基準の付録 A、ドメイン 11 を参照してくだ さい。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS は、外部の認定機関および独立監査人と連携し、コンプライアンスフレームワークへの準拠を確認および検証しています。AWS SOC レポートには、AWS が実行している具体的な物理的セキュリティ統制活動に関する詳細情報が記載されています。詳細については、ISO 27001 基準の付録 A、ドメイン 11 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
3	3.2	3.2.1	(3)	(c)	職員等は、利用する区域について区域情報セキュリティ責任者が定めた対策に従って利用すること。また、職員等が機関等外の者を立ち入らせる際には、当該機関等外の者にも当該区域で定められた対策に従って利用させること。	適合可能	・職員等は、AWSクラウドを利用する場合も、AWSクラウドを利用しない従来の情報システムと同様に、利用する区域について区域情報セキュリティ責任者が定めた対策に従って利用する必要がある。 [留意事項] ・AWSが取得しているISO27001等の認証やSOCレポートで、AWSのセキュリティ統制を確認の上、AWSクラウド利用が可能であるか判断する。 ・AWSクラウドを利用して業務を実施する区域などユーザー側で管理すべき区域においては、当該区域のセキュリティ対策を定め利用することに留意する。	・AWSはISO27001などの認定に準拠し、情報セキュリティフレームワーク、ポリシーを制定しており、利用者は、これらの認証を取得していることを確認可能である。 ・利用者は、AWSのセキュリティ統制について、SOCレポートにて独立監査人によって保証されていることを確認可能である。	AWS は、外部の認定機関および独立監査人と連携し、コンプライアンスフレームワークへの準拠を確認および検証しています。AWS SOC レポートには、AWS が実行している具体的な物理的セキュリティ統制活動に関する詳細情報が記載されています。詳細については、ISO 27001 基準の付録 A、ドメイン 11 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf Amazon の統制環境は、当社の最上層部で開始されます。役員とシニアリーダーは、当社のカラーと中心的な価値を規定する際、重要な役割を担っています。各従業員には当社の業務行動倫理規定が配布され、定期的なトレーニングを受けます。作成したポリシーを従業員が理解し、従うために、コンプライアンス監査が実施されます。詳細については、AWS リスクとコンプライアンスホワイトペーパー (http://aws.amazon.com/compliance) を参照してください。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS はお客様に ISO 27001 認定を提供しています。ISO 27001 認定は特に AWS ISMS に焦点を合わせており、AWS の内部プロセスがどのように ISO 基準に従っているかを測定します。認定とは、サードパーティーによる承認を受けた独立監査機関が AWS のプロセスおよびコントロールを評価し、ISO 27001 認定基準に沿って運用されていることを検証したことを意味します。詳細については、AWS Compliance ISO 27001 FAQ ウェブサイトを参照してください。 http://aws.amazon.com/compliance/iso-27001-faqs/。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS は、情報および関連技術のための統制目標 (COBIT) フレームワークに基づいて情報セキュリティフレームワークとポリシーを制定していて、ISO 27002 統制、米国公認会計士協会 (AICPA) の信頼提供の原則 (Trust Services Principles)、PCI DSS 3.1 版、および米国国立標準技術研究所 (NIST) 出版物 800-53 改訂 3 (連邦情報システム向けの推奨セキュリティ管理) に基づいて ISO 27001 認定可能なフレームワークを実質的に統合しています。 AWS は、ISO 27001 基準に合わせてサードパーティーとの関係を管理しています。 AWS サードパーティーの要件は、PCI DSS、ISO 27001、および FedRAMP への準拠のため、監査中に外部の独立監査人によって確認されます。 AWS コンプライアンスプログラムに関する情報は、http://aws.amazon.com/compliance/ のウェブサイトに一般公開されています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS は、従業員にセキュリティポリシーおよびセキュリティトレーニングを提供することで、情報セキュリティに関する役割と責任について教育しています。 Amazon の基準またはプロトコルに違反した従業員は調査され、適切な懲戒 (警告、業績計画、停職、解雇など) が実施されます。 詳細については、次のウェブサイトで入手可能な AWS クラウドセキュリティホワイトペーパーを参照してください。http://aws.amazon.com/security。詳細については、ISO 27001 基準の付録 A、ドメイン 7 を参照してください。AWS は、 ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf
4	外部委託								
4	4.1	外部委託							
4	4.1	4.1.1	外部委託						
4	4.1	4.1.1	(1)	外部委託に係る規定の整備					
4	4.1	4.1.1	(1)	(a)	統括情報セキュリティ責任者は、外部委託に係る以下の内容を含む規定を整備すること。	対象外			
4	4.1	4.1.1	(1)	(a)	(ア) 委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準（以下本款において「委託判断基準」という。）	対象外			
4	4.1	4.1.1	(1)	(a)	(イ) 委託先の選定基準	対象外			
4	4.1	4.1.1	(2)	外部委託に係る契約					
4	4.1	4.1.1	(2)	(a)	情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託判断基準に従って外部委託を実施すること。	対象外			
4	4.1	4.1.1	(2)	(b)	情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含めること。	対象外			
4	4.1	4.1.1	(2)	(b)	(ア) 委託先に提供する情報の委託先における目的外利用の禁止	対象外			
4	4.1	4.1.1	(2)	(b)	(イ) 委託先における情報セキュリティ対策の実施内容及び管理体制	対象外			
4	4.1	4.1.1	(2)	(b)	(ウ) 委託事業の実施に当たり、委託先企業若しくはその従業員、再委託先又はその他の者によって、機関等の意図せざる変更が加えられないための管理体制	対象外			
4	4.1	4.1.1	(2)	(b)	(エ) 委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供	対象外			
4	4.1	4.1.1	(2)	(b)	(オ) 情報セキュリティインシデントへの対処方法	対象外			
4	4.1	4.1.1	(2)	(b)	(カ) 情報セキュリティ対策その他の契約の履行状況の確認方法	対象外			
4	4.1	4.1.1	(2)	(b)	(キ) 情報セキュリティ対策の履行が不十分な場合の対処方法	対象外			
4	4.1	4.1.1	(2)	(c)	情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託する業務において取り扱う情報の格付等を勘案し、必要に応じて以下の内容を仕様に含めること。	対象外			
4	4.1	4.1.1	(2)	(c)	(ア) 情報セキュリティ監査の受入れ	対象外			
4	4.1	4.1.1	(2)	(c)	(イ) サービスレベルの保証	対象外			
4	4.1	4.1.1	(2)	(d)	情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、上記(b)(c)の措置の実施を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を機関等に提供し、機関等の承認を受けるよう、仕様内容に含めること。また、委託判断基準及び委託先の選定基準に従って再委託の承認の可否を判断すること。	対象外			
4	4.1	4.1.1	(3)	外部委託における対策の実施					
4	4.1	4.1.1	(3)	(a)	情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、契約に基づき、委託先における情報セキュリティ対策の履行状況を確認すること。	対象外			
4	4.1	4.1.1	(3)	(b)	情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合は、委託事業を一時中断するなどの必要な措置を講じた上で、契約に基づく対処を委託先に講じさせること。	対象外			

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
4	4.1	4.1.1	(3)	(c)	情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託した業務の終了時に、委託先において取り扱われた情報が確実に返却、又は抹消されたことを確認すること。	対象外			
4	4.1	4.1.1	(4)	外部委託における情報の取扱い					
4	4.1	4.1.1	(4)	(a)	職員等は、委託先への情報の提供等において、以下の事項を遵守すること。	対象外			
4	4.1	4.1.1	(4)	(a)	(ア) 委託先に要保護情報を提供する場合は、提供する情報を必要最小限とし、あらかじめ定められた安全な受渡し方法により提供すること。	対象外			
4	4.1	4.1.1	(4)	(a)	(イ) 提供した要保護情報が委託先において不要になった場合は、これを確実に返却又は抹消させること。	対象外			
4	4.1	4.1.1	(4)	(a)	(ウ) 委託業務において、情報セキュリティインシデント、情報の目的外利用等を認知した場合は、速やかに情報システムセキュリティ責任者又は課室情報セキュリティ責任者に報告すること。	対象外			
4	4.1	4.1.2	約款による外部サービスの利用						
4	4.1	4.1.2	(1)	約款による外部サービスの利用に係る規定の整備					
4	4.1	4.1.2	(1)	(a)	統括情報セキュリティ責任者は、以下を含む約款による外部サービスの利用に関する規定を整備すること。また、当該サービスの利用において要機密情報が取り扱われないよう規定すること。	対象外			
4	4.1	4.1.2	(1)	(a)	(ア) 約款による外部サービスを利用してよい業務の範囲	対象外			
4	4.1	4.1.2	(1)	(a)	(イ) 業務に利用できる約款による外部サービス	対象外			
4	4.1	4.1.2	(1)	(a)	(ウ) 利用手続及び運用手順	対象外			
4	4.1	4.1.2	(1)	(b)	情報セキュリティ責任者は、約款による外部サービスを利用する場合は、利用するサービスごとの責任者を定めること。	対象外			
4	4.1	4.1.2	(2)	約款による外部サービスの利用における対策の実施					
4	4.1	4.1.2	(2)	(a)	職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用すること。	対象外			
4	4.1	4.1.3	ソーシャルメディアサービスによる情報発信						
4	4.1	4.1.3	(1)	ソーシャルメディアサービスによる情報発信時の対策					
4	4.1	4.1.3	(1)	(a)	統括情報セキュリティ責任者は、機関等が管理するアカウントでソーシャルメディアサービスを利用することを前提として、以下を含む情報セキュリティ対策に関する運用手順等を定めること。また、当該サービスの利用において要機密情報が取り扱われないよう規定すること。	対象外			
4	4.1	4.1.3	(1)	(a)	(ア) 機関等のアカウントによる情報発信が実際の機関等のものであると明らかとするために、アカウントの運用組織を明示するなどの方法でなりすましへの対策を講ずること。	対象外			
4	4.1	4.1.3	(1)	(a)	(イ) パスワード等の主体認証情報を適切に管理するなどの方法で不正アクセスへの対策を講ずること。	対象外			
4	4.1	4.1.3	(1)	(b)	情報セキュリティ責任者は、機関等において情報発信のためにソーシャルメディアサービスを利用する場合は、利用するソーシャルメディアサービスごとの責任者を定めること。	対象外			
4	4.1	4.1.3	(1)	(c)	職員等は、要安定情報の国民への提供にソーシャルメディアサービスを用いる場合は、機関等の自己管理ウェブサイトに当該情報を掲載して参照可能とすること。	対象外			
4	4.1	4.1.4	クラウドサービスの利用						
4	4.1	4.1.4	(1)	クラウドサービスの利用における対策					
4	4.1	4.1.4	(1)	(a)	情報システムセキュリティ責任者は、クラウドサービス（民間事業者が提供するものに限らず、機関等が自ら提供するものを含む。以下同じ。）を利用するに当たり、取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断すること。	適合可能	・情報システムセキュリティ責任者は、クラウドサービス（民間事業者が提供するものに限らず、機関等が自ら提供するものを含む。）を利用するに当たり、取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断する必要がある。 [留意事項] ・AWSが取得しているISO27001等の認証やSOCレポートで、AWSのセキュリティ統制を確認の上、AWSクラウド利用が可能であるか判断する。 ・クラウドサービスを利用するにあたっては、クラウドサービスが提供する責任範囲を理解した上で、情報の取り扱いを委ねることになるのか利用者が制御できるのかを確認する必要があることに留意する。 ・AWSクラウドを利用する場合は、情報の取扱は利用者側の責任であり情報システムセキュリティ責任者が、従来どおりのセキュリティ対策を行う必要があることに留意する。	・AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、Amazonの IT 統制環境に関する情報やリスクおよびコンプライアンスプログラムに関する情報を提供しており、AWSクラウドの利用者はこれらの情報を検証し、自身の管理フレームワークにAWSの統制を組み込むことができる。 ・利用者は、AWSの統制内容について、SOCレポートにて独立監査人によって保証されていることを確認可能である。 ・AWSは、ISO27001に準拠し情報セキュリティフレームワークとポリシーを制定しており、利用者はこれらの認証を取得していることを確認可能である。	AWS にデプロイされている部分については、AWS がそのテクノロジの物理コンポーネントを統制します。その他の部分は、接続ポイントや送信の統制を含め、お客様がすべてを所有し、統制します。AWS で定めている統制の内容と、効率的に運用する方法について理解できるように、AWS では SOC 1 Type II レポートを発行し、EC2、S3、VPC を中心とした定義済みの統制、ならびに詳細な物理セキュリティおよび環境統制を公表しています。これらの統制の定義は、ほとんどのお客様のニーズを満たします。AWS と機密保持契約を結んでいる AWS のお客様は、SOC 1 Type II レポートのコピーを要求できます。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、当社の IT 統制環境に関する幅広い情報をお客様にご提供しています。本文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様にご理解いただくことをお手伝いするためのものです。この情報はまた、お客様の拡張された IT 環境内の統制が効果的に機能しているかどうかを明らかにし、検証するのにも有用です。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS では、お客様の管理フレームワークに AWS 統制を組み込むことができるように、リスクおよびコンプライアンスプログラムに関する情報を提供しています。この情報をもとに、AWS に関する統制と管理フレームワーク全体を文書化し、フレームワークの重要な部分としてご利用いただけます。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS マネジメントは、リスクを緩和または管理するためのリスク特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、戦略的事業計画を再評価します。このプロセスでは、マネジメントがその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。 さらに、AWS 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標 (COBIT) フレームワークに基づいて、情報セキュリティフレームワークとポリシーを規定しました。また、ISO 27002 規格、米国公認会計士協会 (AICPA) の信頼提供の原則 (Trust Services Principles)、PCI DSS v3.0、および米国国立標準技術研究所 (NIST) 出版物 800-53 Rev 3 (連邦政府情報システムにおける推奨セキュリティ統制) に基づいて、 ISO 27001 認定対応フレームワークを実質的に統合しました。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実行します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
4	4.1	4.1.4	(1)	(b)	情報システムセキュリティ責任者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定すること。	適合可能	・情報システムセキュリティ責任者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定する必要がある。 [留意事項] ・AWSクラウドを利用する場合は、法令が適用される範囲、情報システムへの影響度、顕在化する確度などを判断し、適正な選定条件を指定する必要があることに留意する。 ・AWSクラウドを利用する場合は、必要に応じて、東京リージョンを指定し、日本法準拠および東京地裁に変更することを検討する。	・AWSカスタマーアグリーメントの準拠法は、本契約およびサービス利用者とアマゾンの間に生じるすべての種類の紛争については、アメリカ合衆国ワシントン州法、紛争解決手段はアメリカ合衆国仲裁協会の規則に基づく手続きと規定されているが、AWSは、日本の利用者に対して、リクエストに応じて日本法準拠および東京地裁への変更を提示している。 ・AWSでは、データとサーバーを配置する物理的なリージョンをAWS の利用者が指定することができるため、情報を日本に保存することができる。 ・AWSクラウドでは、利用者がデータの統制と所有権を有しており、AWS上のリソースについてアクセス権、暗号化などのセキュリティ対策を施すことが可能である。	データとサーバーを配置する物理的なリージョンは、AWS のお客様が指定します。S3 データオブジェクトのデータレプリケーションは、データが保存されているリージョンのクラスタ内で実行され、他のリージョンの他のデータセンタークラスタにはレプリケートされません。データとサーバーを配置する物理的なリージョンは、AWS のお客様が指定します。AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しないものとします。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS のお客様は、お客様のデータの統制と所有権を保持します。AWS はお客様のプライバシー保護を慎重に考慮し、AWS が準拠する必要がある法的処置の要求についても注意深く判断しています。AWS は、法的処置による命令に確実な根拠がないと判断した場合は、その命令にためらわずに異議を申し立てます。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf 13.11 準拠法、裁判地　本契約およびサービス利用者とアマゾンの間に生じるすべての種類の紛争は、法の抵触に関する規則の適用は除外して、アメリカ合衆国ワシントン州法に準拠する。国際物品売買契約に関する国際連合条約は本契約には適用されない。 13.12 紛争　サービス利用者による提供される本サービス内容の利用に関連する、または AWS が販売もしくは配布する製品もしくはサービスに関連する紛争またはクレームは全て、裁判所ではなく拘束力のある仲裁により解決される。ただし、サービス利用者は、サービス利用者のクレームが適格要件を満たす場合に少額裁判所（small claims court）にクレームを申し立てることができる。連邦仲裁法および連邦仲裁規範が本契約に適用される。仲裁には判事も陪審員もおらず、仲裁の裁定に対する裁判所の審査は限定される。しかし、仲裁人は裁判所と同様の損害賠償および救済（差し止めによる救済、宣言的救済または法定損害賠償を含む）を個別事案ごとに裁定することができ、裁判所がそうであるのと同様に本契約の条項に従わなくてはならない。仲裁手続きを開始するために、サービス利用者は、アマゾンの登録代理人である Corporation Service Company（300 Deschutes Way SW, Suite 304, Tumwater, WA 98501）宛てに、仲裁を要請しサービス利用者のクレームを説明する書簡を送付しなければならない。仲裁は、米国仲裁協会（AAA）によって、www.adr.org 上で、または 1-800-778-7879 に電話することによって入手可能である AAA の規則に基づき行われる。申立て手数料、事務手数料および仲裁人手数料の支払いは、AAA の規則に準拠する。アマゾンは、仲裁人がクレームについて根拠がないと判断しない限り、総額 10,000 ドル未満のクレーム手数料を払い戻す。アマゾンは、仲裁人がクレームについて根拠がないと判断しない限り、仲裁の弁護士費用および経費を求めない。サービス利用者は、書面提出に基づいて、電話によって、または相互に合意した場所において、仲裁を行うことを選択できる。アマゾンおよびサービス利用者は、紛争解決手続を個別事案ごとに行い、集団訴訟、統合訴訟または代表訴訟を行わないことに合意する。もし何らかの理由によってクレームが仲裁ではなく裁判所で進行する場合は、アマゾンおよびサービス利用者は陪審裁判の権利を放棄する。第 8.5 項を条件として、アマゾンおよびサービス利用者は双方とも、サービス利用者またはアマゾンが、知的財産権の侵害またはその他の不正利用を差し止めるため、裁判所に訴訟を提起できることに合意する。 詳細に関してはhttps://aws.amazon.com/jp/agreement/をご参照下さい。 ●セキュリティ: お客様は、自分のカスタマーコンテンツの安全をどのように確保するかを選択できます。私たちはお客様のために、移動中または保管中のコンテンツの強力な暗号化機能を準備しています。暗号化キーをお客様ご自身で管理するオプションも用意されています。 ●カスタマーコンテンツの開示: 法令、または政府機関もしくは規制当局による有効かつ拘束力のある命令を遵守するために必要な場合を除き、お客様のコンテンツを開示することはありません。そうすることが禁止されている場合または Amazon の製品もしくはサービスの利用に関連した違法行為の存在を明確に示すものがある場合を除き、Amazon ではカスタマーコンテンツの開示に先立ってお客様に通知し、お客様が開示からの保護を求められるようにします。 詳細に関しては「AWSウェブサイトのデータプライバシー」をご参照下さい。 https://aws.amazon.com/jp/compliance/data-privacy-faq/

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
4	4.1	4.1.4	(1)	(c)	情報システムセキュリティ責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件とすること。	適合可能	・情報システムセキュリティ責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、必要に応じて委託先を選定する際の要件とする必要がある。 [留意事項] ・業務の移行は情報システムセキュリティ責任者が実施する必要があることに留意する。業務の移行を円滑に行うために、クラウドサービスの選定条件として、必要に応じて、以下に例示する要件を含めることを検討する。 -クラウドサービスの中断及び終了時の事前告知の方法・期限 -クラウドサービスで構築した情報システムやデータを移行するための機能の有無 ・AWSクラウドのAMIをエクスポートし、AWSクラウド外に移行する場合は、ライセンス制限などにより移行できない場合があるため留意が必要である。	・AWSは、必要に応じて利用者が自身のデータをAWSクラウドの内外に出し入れすることを許可しており、クラウドサービス終了時にデータをAWSクラウド以外に出力することが可能である。 ・AWSは、以下のような機能を提供しており、サービス中断時及び終了時に利用者がAWSクラウド上に構築した情報システム及び格納したデータを移行することが可能である。 -Amazon マシンイメージ (AMI)を作成し、出力する機能を提供する。 -AWS Import/ExportなどAWSストレージからデータを出力する機能を提供する。 ・AWSは、重要なサービスの変更または中止を行う場合、利用者に通知を行っている。	お客様は、お客様のデータの統制と所有権を保持します。お客様は、AMI をエクスポートして、施設内または別のプロバイダーで使用できます (ただし、ソフトウェアのライセンス制限に従います)。詳細については、AWS セキュリティプロセスの概要ホワイトペーパー (http://aws.amazon.com/security) を参照してください。 AWS では、必要に応じてお客様がデータを AWS ストレージから出し入れすることを許可しています。S3 用 AWS Import/Export サービスでは、転送用のポータブル記憶装置を使用して、AWS 内外への大容量データの転送を高速化できます。AWS では、お客様がご自分のテープバックアップサービスプロバイダーを使用してテープへのバックアップを実行することを許可しています。ただし、AWS ではテープへのバックアップサービスを提供していません。 AWS データセンターは、世界のさまざまなリージョンにクラスター化されて構築されています。すべてのデータセンターはオンラインで顧客にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、影響を受けたエリアから顧客データが移動されます。重要なアプリケーションは N+1 原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。AWS は、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。各アベイラビリティーゾーンは、独立した障害ゾーンとして設計されています。つまり、アベイラビリティーゾーンは、一般的な都市地域内で物理的に分離されており、洪水の影響が及ばないような場所にあります (洪水地域の分類はリージョンによって異なります)。個別の無停電電源装置 (UPS) やオンサイトのバックアップ生成施設に加え、シングルポイントの障害の可能性を減らすために、別々の電力供給施設から異なる配管網を経由して、個別に電力供給を行っています。これらはすべて、冗長的に、複数の Tier-1 プロバイダーに接続されています。顧客は AWS の使用量を計画しながら、複数のリージョンやアベイラビリティーゾーンを利用する必要があります。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配信することによって、自然災害やシステム障害など、ほとんどの障害モードに対して、その可用性を保つことができます。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf 2. 変更 2.1 提供される本サービス内容の変更　アマゾンは、随時、（提供される本サービス内容全体を含めて）提供される本サービス内容のいずれの部分についても変更、中止、廃止し、あるいは提供される本サービス内容の属性もしくは機能を変更または削除することができるものとする。提供される本サービス内容の重要な変更または中止を行う場合には、アマゾンは、サービス利用者に対して通知する。 2.2 API の変更　アマゾンは、随時、本サービスの API を変更、中止または廃止することができるものとするが、変更、中止または廃止から 12 ヶ月間は、変更、中止または廃止された API の以前のバージョンのサポートを継続するため商業上合理的な努力をする。ただし、それにより、(a)セキュリティもしくは知的財産の問題が生じる場合、(b)経済的もしくは技術的に負担が大きい場合、または(c)法律もしくは政府機関の要請を遵守する必要がある場合を除く。 2.3 サービスレベルアグリーメントの変更　アマゾンは、第 12 条に従い、随時、サービスレベルアグリーメントを変更、中止または追加することができるものとする。 7. 契約期間および契約解除 7.1. 契約期間　本契約の期間は、契約発効日に開始し、第7.2項に従って、サービス利用者またはアマゾンにより解除されるまで有効に存続する。 7.2 契約解除 (a) 無理由解除 サービス利用者は、(i)アマゾンへの通知、および(ii)すべての本サービスのためのサービス利用者のアカウントの閉鎖（アカウント閉鎖の手段はアマゾンが提供する。）により、理由を問わず本契約を解除することができる。アマゾンは、サービス利用者に30日前までに通知することにより、理由を問わず本契約を解除することができる。 (b) 正当事由による契約解除 (i) 各当事者による解除 相手方当事者による本契約の重大な不履行または違反があり、違反当事者に対して30日前までに通知をしたが、違反当事者が30日以内に当該重大な不履行または違反を是正しない場合、他方当事者は、正当事由により本契約を解除することができる。 (ii) アマゾンによる解除 アマゾンはさらに、以下の場合には、サービス利用者に対して通知することにより、直ちに本契約を解除することができる。(A)サービス利用者またはエンドユーザーによる作為もしくは不作為の結果、第 6.1 項に定める停止となった場合、(B)提供される本サービス内容を提供するためにアマゾンが使用するソフトウェアその他の技術を提供している第三者パートナーとアマゾンの関係が終了し、解除され、または本サービスの一環としてソフトウェアその他の技術をアマゾンが提供する方法を変更する必要が生じた場合、(C)本サービスの提供により、重大な経済的もしくは技術的な負担、または重大なセキュリティの危険がアマゾンに生じると考えられる場合、(D)法律または政府機関の要請を遵守する必要が生じた場合、または(E)サービス利用者もしくはエンドユーザーによる提供される本サービス内容の利用、またはサービス利用者もしくはエンドユーザーに対するアマゾンによる本サービスの提供が、法律上、規制上の理由で、非現実的または実行不能であるとアマゾンが判断する場合。 7.3. 契約解除の効果 (a) 全般 本契約が解除された場合には、以下の規定が適用される。 (i) 本契約に基づくサービス利用者のすべての権利は直ちに終了する。 (ii) サービス利用者は、解除日までに生じたすべての料金等、および解除日以降に完了される進行中の作業の料金等を支払う責任を引き続き負う。 (iii) サービス利用者は、自己が保有する AWS コンテンツのすべてを直ちに返却するか、アマゾンの指示がある場合にはそれを破棄するものとする。 (iv) 第 4.1 項、第 5.2 項、第 7.3 項、第 8 条(第 8.4 項においてサービス利用者に付与されるライセンスを除く）、第 9 条、第 10 条、第 11 条、第 13 条および第 14 条は、その条件に従い引き続き適用される。 (b) 契約解除後の支援 第 7.2 項(b)に従ってアマゾンがサービス利用者による提供される本サービス内容の利用を解除する場合を除き、解除後 30 日間は、以下の規定が適用される。 (i) アマゾンは、解除にかかわらず、いかなるサービス利用者コンテンツも消去しない。 (ii) サービス利用者が、契約解除後の提供される本サービス内容の利用のための料金等およびその他の支払額のすべてを支払っている場合に限り、サービス利用者はサービス利用者コンテンツを本サービスから取り出すことができる。 (iii) アマゾンは、アマゾンがすべての顧客に対して一般的に提供するものと同様の、契約解除後のデータ取り出しの支援をサービス利用者に対して提供する。 契約解除後のアマゾンによるその他の支援は、サービス利用者とアマゾンの相互合意に従う。 12.本契約の変更 アマゾンは、AWS サイトに改訂版を掲載するか、第 13.7 項に従いその他の方法でサービス利用者に通知することにより、本契約（アマゾン規約を含む。）をいつでも変更することができる。但し、アマゾンは、サービスレベルアグリーメントのいずれかに対する重大な変更については、第 13.7 項に従い遅くとも 90 日前までにこれを通知する。変更された条件は、AWS サイトへの掲載時、またはアマゾンがサービス利用者に電子メールで通知する場合は電子メールの記載に従って、また、サービスレベルアグリーメントに対する重大な変更に関しては 90 日前通知を条件として、発効する。本契約の変更の発効日以降に引き続き提供される本サービス内容を利用した場合には、サービス利用者は、変更後の条件に拘束されることに同意したものとする。本契約の変更を知るために AWS サイトを定期的に閲覧することはサービス利用者の責任である。アマゾンによる本契約の最終変更日は、本契約の末尾に記載されているとおりである。 詳細に関してはhttps://aws.amazon.com/jp/agreement/をご参照下さい。

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
4	4.1	4.1.4	(1)	(d)	情報システムセキュリティ責任者は、クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定めること。	適合可能	・情報システムセキュリティ責任者は、クラウドサービスを利用する場合は、クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定める必要がある。 [留意事項] ・クラウドサービスを利用する場合は、クラウドサービスの責任範囲を確認し、利用者の責任範囲については従来通りの対策を行う必要があることに留意する。 ・AWSのサービス仕様や制約事項を確認し、要件を満たさない場合は、要求事項を満たす対策を行う必要があることに留意する。 ・AWSクラウドが提供するサービスの各種設定及び構成は利用者が設計・設定・運用する必要があることに留意する。 ・具体的なセキュリティ要件の確保という点では、AWSが提供するVPC, WAF, IAM, SecurityGroup, 暗号化等の各種セキュリティ関連サービスやオプションの機能性を確認する必要がある。 ・AWSが取得しているISO27001等の認証やSOCレポートで、AWSの統制環境を確認の上、AWSクラウド利用が可能であるか判断する。	・利用者は、AWSの統制内容について、SOCレポートにて独立監査人によって保証されていることを確認可能である。 ・AWS内部のネットワークアーキテクチャは、ISO27001に準拠し作成されており、利用者はこれらの認証を取得していることを確認可能である。	AWS にデプロイされている部分については、AWS がそのテクノロジの物理コンポーネントを統制します。その他の部分は、接続ポイントや送信の統制を含め、お客様がすべてを所有し、統制します。AWS で定めている統制の内容と、効率的に運用する方法について理解できるように、AWS では SOC 1 Type II レポートを発行し、EC2、S3、VPC を中心とした定義済みの統制、ならびに詳細な物理セキュリティおよび環境統制を公表しています。これらの統制の定義は、ほとんどのお客様のニーズを満たします。AWS と機密保持契約を結んでいる AWS のお客様は、SOC 1 Type II レポートのコピーを要求できます。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS のお客様は、お客様が定義した要件に従って、お客様のネットワークセグメントを管理する責任を有します。 AWS 内部では、AWS のネットワークセグメントは ISO 27001 基準に合わせて作成されています。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf ・ファイアウォールや他の境界デバイスなどのネットワークデバイスは、ネットワークの外部境界およびネットワーク内の主要な内部境界で通信を監視および制御するために用意されています。これらの境界デバイスでは、ルールセット、アクセスコントロールリスト（ACL）、および設定が採用され、強制的に特定の情報システムサービスに情報が流れます。 ACL、つまりトラフィックフローのポリシーは、各マネージドインターフェイスに設定され、トラフィックの流れを監視して流します。ACL ポリシーは Amazon 情報セキュリティによって承認されます。これらのポリシーは、AWS の ACL 管理ツールを使用して自動的にプッシュされ、確実にマネージドインターフェイスで最新の ACL が実行されます。 ・AWS では、インバウンドとアウトバウンドの通信およびネットワークトラフィックをより包括的に監視することを考え、限られた数のクラウドへのアクセスポイントを戦略的に設置しました。このようなお客様のアクセスポイントは API エンドポイントと呼ばれ、安全な HTTP アクセス（HTTPS）を許可します。これにより、ご利用のストレージまたは AWS 内のコンピューティングインスタンスとの安全な通信セッションを確立できます。FIPS 暗号要件への準拠を必要とするお客様をサポートするために、AWS GovCloud（米国）内の SSL 終端ロードバランサーは、FIPS 140-2 に準拠しています。 さらに、AWS は、インターネットサービスプロバイダ（ISP）とのインターフェイス通信を管理するためのネットワークデバイスを実装しました。AWS ネットワークのインターネット側のそれぞれの境界では、複数の通信サービスへの重複する接続を採用しています。これらの接続にはそれぞれ、専用ネットワークデバイスがあります。 ・HTTP または Secure Sockets Layer（SSL）を使用した HTTPS を介して AWS のアクセスポイントに接続できます。SSL は、傍受、改ざん、およびメッセージの偽造から保護するように設計された暗号プロトコルです。 ネットワークセキュリティの追加レイヤーが必要なお客様のために、AWS では Amazon Virtual Private Cloud（VPC）を提供しています。これにより、AWS クラウド内にプライベートサブネットが提供され、Amazon VPC とデータセンターの間に 暗号化されたトンネルを提供する IPsec 仮想プライベートネットワーク（VPN）のデバイスを使用できるようになります。 VPC の設定オプションの詳細については、後の「Amazon Virtual Private Cloud（Amazon VPC）のセキュリティ」のセクションをご覧ください。 詳細に関しては「セキュリティプロセスの概要 （2014年11月版）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf
4	4.1	4.1.4	(1)	(e)	情報システムセキュリティ責任者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断すること。	適合可能	情報システムセキュリティ責任者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断する必要がある。 [留意事項] ・AWSから提供される各種セキュリティやコンプライアンスに関連するホワイトペーパーや、第三者による客観的な監査によって取得された認証や監査レポートを元に判断する必要があることに留意する。	・AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、Amazonの IT 統制環境に関する幅広い情報を提供しており、AWSクラウドの利用者はこれらの情報を検証することが可能である。	AWS は、サードパーティーによる証明、認定、Service Organization Controls (SOC) レポートなどの関連するコンプライアンスレポートを、NDA に従ってお客様に直接提供しています。 AWS ISO 27001 認定は次のウェブサイトからダウンロードできます。http://d0.awsstatic.com/certifications/iso_27001_global_certification.pdf.AWS SOC 3 レポートは次のウェブサイトからダウンロードできます。https://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf. AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします (お客様のインスタンスはこのスキャンの対象外です)。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、脆弱性に対する外部からの脅威の査定が、独立系のセキュリティ会社によって定期的に実行されます。これらの査定に起因する発見や推奨事項は、分類整理されて AWS 上層部に報告されます。 さらに、AWS 統制環境は、通常の内部的および外部的監査およびリスク評価によって規定されています。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS は、ホワイトペーパー、レポート、認定、認証評価、およびその他のサードパーティによる証明を通して、当社の IT統制環境に関するさまざまな情報をお客様に提供しています。詳細については、ウェブサイト（http://aws.amazon.com/compliance/）で入手可能なリスクと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。 詳細に関しては「セキュリティプロセスの概要 （2014年11月版）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf AWS マネジメントは、リスクを緩和または管理するためのリスク特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、戦略的事業計画を再評価します。このプロセスでは、マネジメントがその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。 さらに、AWS 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標 (COBIT) フレームワークに基づいて、情報セキュリティフレームワークとポリシーを規定しました。また、ISO 27002 規格、米国公認会計士協会 (AICPA) の信頼提供の原則 (Trust Services Principles)、PCI DSS v3.0、および米国国立標準技術研究所 (NIST) 出版物 800-53 Rev 3 (連邦政府情報システムにおける推奨セキュリティ統制) に基づいて、 ISO 27001 認定対応フレームワークを実質的に統合しました。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実行します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf
5	情報システムのライフサイクル								
5	5.1	情報システムに係る文書等の整備							
5	5.1	5.1.1	情報システムに係る台帳等の整備						
5	5.1	5.1.1	(1)	情報システム台帳の整備					
5	5.1	5.1.1	(1)	(a)	統括情報セキュリティ責任者は、全ての情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳に整備すること。	対象外			
5	5.1	5.1.1	(1)	(b)	情報システムセキュリティ責任者は、情報システムを新規に構築し、又は更改する際には、当該情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について統括情報セキュリティ責任者に報告すること。	対象外			
5	5.1	5.1.1	(2)	情報システム関連文書の整備					
5	5.1	5.1.1	(2)	(a)	情報システムセキュリティ責任者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を網羅した情報システム関連文書を整備すること。	対象外			

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
5	5.1	5.1.1	(2)	(a)	(ア) 情報システムを構成するサーバ装置及び端末関連情報	対象外			
5	5.1	5.1.1	(2)	(a)	(イ) 情報システムを構成する通信回線及び通信回線装置関連情報	対象外			
5	5.1	5.1.1	(2)	(a)	(ウ) 情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順	対象外			
5	5.1	5.1.1	(2)	(a)	(エ) 情報セキュリティインシデントを認知した際の対処手順	対象外			
5	5.1	5.1.2	機器等の調達に係る規定の整備						
5	5.1	5.1.2	(1)	機器等の調達に係る規定の整備					
5	5.1	5.1.2	(1)	(a)	統括情報セキュリティ責任者は、機器等の選定基準を整備すること。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を機関等が確認できることを加えること。	適合可能	・統括情報セキュリティ責任者は、機器等を調達する場合は、AWSクラウドを利用する場合も、AWSクラウドを利用しない従来の情報システムと同様に選定基準を整備する必要がある。 [留意事項] ・AWSが取得しているISO27001等の認証やSOCレポートで、AWSの機器選定基準やライフサイクルにおける不正な変更が加えらない管理が実施されていること確認の上、AWSクラウド利用が可能であるか判断する。	・AWSはISO27001などの認定に準拠し、ソフトウェアおよびハードウェアの調達、追跡および監視を行っており、利用者は、これらの認証を取得していることを確認可能である。 ・利用者は、AWS のサードパーティー管理プロセスについて、SOCレポートにて独立監査人によって保証されていることを確認可能である。	ISO 27001 基準に合わせて、AWS の担当者が AWS 専有インベントリ管理ツールを使用して、AWS ハードウェアの資産に所有者を割り当て、追跡および監視を行っています。AWS の調達およびサプライチェーンチームは、すべての AWS サプライヤとの関係を維持しています。 詳細については、ISO 27001 基準の付録 A、ドメイン 7.1 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS では、主要なサードパーティーサプライヤーと正式な契約を締結し、ビジネスでの関係に合わせた適切なリレーションシップ管理メカニズムを実装しています。 AWS のサードパーティー管理プロセスは、SOC および ISO 27001 への AWS の継続的な準拠の一環として、独立監査人によって確認されます。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS のお客様は、コンテンツのアセット管理に責任を負い、それを実装および運用します。お客様の物理アセットに在庫追跡システムを導入するのは、お客様の責任となります。 AWS データセンターの環境については、サーバー、ラック、ネットワークデバイス、ハードドライブ、システムハードウェアコンポーネント、および建築資材といった新しい情報システムコンポーネントがデータセンターに出荷される場合、必ずデータセンターマネージャーが事前に承認する必要があり、納品時にはデータセンターマネージャーに通知する必要があります。物品は各 AWS データセンターの搬入口に配送されます。AWS の正社員は、破損や梱包が開封された痕跡がないことを検査し、署名します。物品は配達時に、AWS のアセット管理システムとデバイス在庫追跡システムによりスキャンおよび記録されます。 受領された物品は、データセンターのフロアに設置されるまで、データセンター内の機器保管室に置かれます。機器保管室に入るには、ID カードの読み取りと PIN の入力が必要です。物品がデータセンターから搬出される場合、搬出の承認を受ける前に、その物品のスキャン、使用履歴の追跡、データの消去が行われます。 AWS のアセット管理のプロセスと手順は、PCI DSS、ISO 27001、および FedRAMP のコンプライアンスの監査時に、社外の独立監査人によって確認されます。 詳細に関してはhttps://aws.amazon.com/jp/compliance/mpaa/をご参照下さい。
5	5.1	5.1.2	(1)	(b)	統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。	適合可能	・統括情報セキュリティ責任者は、機器等を調達する場合は、AWSクラウドを利用する場合も、AWSクラウドを利用しない従来の情報システムと同様に情報セキュリティ対策の視点を加味して確認・検査手続を整備する必要がある。 [留意事項] ・AWSが取得しているISO27001等の認証やSOCレポートで、AWSの機器等の納入時の確認・検査手続きの整備内容を確認の上、AWSクラウド利用が可能であるか判断する。	・AWSは、ISO27001などの認定に準拠し、AWSデータセンター内の物理的機器等の資産管理を行っており、利用者は、これらの認証を取得していることを確認可能である。 ・利用者は、AWS の資産管理プロセスと手順について、SOCレポートにて独立監査人によって保証されていることを確認可能である。	ISO 27001 基準に合わせて、AWS の担当者が AWS 専有インベントリ管理ツールを使用して、AWS ハードウェアの資産に所有者を割り当て、追跡および監視を行っています。AWS の調達およびサプライチェーンチームは、すべての AWS サプライヤとの関係を維持しています。 詳細については、ISO 27001 基準の付録 A、ドメイン 7.1 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS では、主要なサードパーティーサプライヤーと正式な契約を締結し、ビジネスでの関係に合わせた適切なリレーションシップ管理メカニズムを実装しています。 AWS のサードパーティー管理プロセスは、SOC および ISO 27001 への AWS の継続的な準拠の一環として、独立監査人によって確認されます。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS のお客様は、コンテンツのアセット管理に責任を負い、それを実装および運用します。お客様の物理アセットに在庫追跡システムを導入するのは、お客様の責任となります。 AWS データセンターの環境については、サーバー、ラック、ネットワークデバイス、ハードドライブ、システムハードウェアコンポーネント、および建築資材といった新しい情報システムコンポーネントがデータセンターに出荷される場合、必ずデータセンターマネージャーが事前に承認する必要があり、納品時にはデータセンターマネージャーに通知する必要があります。物品は各 AWS データセンターの搬入口に配送されます。AWS の正社員は、破損や梱包が開封された痕跡がないことを検査し、署名します。物品は配達時に、AWS のアセット管理システムとデバイス在庫追跡システムによりスキャンおよび記録されます。 受領された物品は、データセンターのフロアに設置されるまで、データセンター内の機器保管室に置かれます。機器保管室に入るには、ID カードの読み取りと PIN の入力が必要です。物品がデータセンターから搬出される場合、搬出の承認を受ける前に、その物品のスキャン、使用履歴の追跡、データの消去が行われます。 AWS のアセット管理のプロセスと手順は、PCI DSS、ISO 27001、および FedRAMP のコンプライアンスの監査時に、社外の独立監査人によって確認されます。 詳細に関してはhttps://aws.amazon.com/jp/compliance/mpaa/をご参照下さい。
5	5.2	情報システムのライフサイクルの各段階における対策							
5	5.2	5.2.1	情報システムの企画・要件定義						
5	5.2	5.2.1	(1)	実施体制の確保					
5	5.2	5.2.1	(1)	(a)	情報システムセキュリティ責任者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を、最高情報セキュリティ責任者に求めること。	対象外	情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を、最高情報セキュリティ責任者に求めることは、クラウドサービス利用有無にかかわらず、情報システムセキュリティ責任者が遵守すべき事項である。	情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を、情報システムを統括する責任者に求めることについては、本リファレンスの説明の対象外。	
5	5.2	5.2.1	(1)	(b)	情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システムを整備し運用管理する機関等が定める運用管理規程等に応じた体制の確保を、最高情報セキュリティ責任者に求めること。	対象外	基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システムを整備し運用管理する府省庁が定める運用管理規程等に応じた体制の整備を、最高情報セキュリティ責任者に求めることは、クラウドサービス利用有無にかかわらず、情報システムセキュリティ責任者が遵守すべき事項である。	基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システムを整備し運用管理する府省庁が定める運用管理規程等に応じた体制の整備を、情報システムを統括する責任者に求めることについては、本リファレンスの説明の対象外。	
5	5.2	5.2.1	(1)	(c)	最高情報セキュリティ責任者は、前二項で求められる体制の確保に際し、情報システムを統括する責任者（情報化統括責任者（CIO））の協力を得ることが必要な場合は、当該情報システムを統括する責任者に当該体制の全部又は一部の整備を求めること。	対象外	前二項で求められる体制の確保に際し、情報システムを統括する責任者（情報化統括責任者（CIO））の協力を得ることが必要な場合は、当該情報システムを統括する責任者に当該体制の全部又は一部の整備を求めることは、クラウドサービス利用有無にかかわらず、最高情報セキュリティ責任者が遵守すべき事項である。	前二項で求められる体制の確保に際し、情報システムを統括する責任者（情報化統括責任者（CIO））の協力を得ることが必要な場合は、当該情報システムを統括する責任者に当該体制の全部又は一部の整備を、最高情報セキュリティ責任者に求めることについては、本リファレンスの説明の対象外。	

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
5	5.2	5.2.1	(2)	情報システムのセキュリティ要件の策定					
5	5.2	5.2.1	(2)	(a)	情報システムセキュリティ責任者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等に基づき、構築する情報システムをインターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することの要否を判断した上で、以下の事項を含む情報システムのセキュリティ要件を策定すること。	対象外	情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等に基づき、構築する情報システムをインターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することの要否を判断した上で、情報システムのセキュリティ要件を策定することは、クラウドサービス利用有無にかかわらず、情報システムセキュリティ責任者が検討すべき事項である。	情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等に基づき、構築する情報システムをインターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することの要否を判断した上で、情報システムのセキュリティ要件を策定することについては、本リファレンスの説明の対象外。	
5	5.2	5.2.1	(2)	(a)	(ア) 情報システムに組み込む主体認証、アクセス制御、権限管理、ログ管理、暗号化機能等のセキュリティ機能要件	対象外	情報システムに組み込む主体認証、アクセス制御、権限管理、ログ管理、暗号化機能等のセキュリティ機能要件を策定することは、クラウドサービス利用有無にかかわらず、情報システムセキュリティ責任者が検討すべき事項である。	情報システムに組み込む主体認証、アクセス制御、権限管理、ログ管理、暗号化機能等のセキュリティ機能要件を策定することについては、本リファレンスの説明の対象外。	
5	5.2	5.2.1	(2)	(a)	(イ) 情報システム運用時の監視等の運用管理機能要件（監視するデータが暗号化されている場合は、必要に応じて復号すること）	対象外	情報システム運用時の監視等の運用管理機能要件を策定することは、クラウドサービス利用有無にかかわらず、情報システムセキュリティ責任者が検討すべき事項である。	情報システム運用時の監視等の運用管理機能要件を策定することについては、本リファレンスの説明の対象外。	
5	5.2	5.2.1	(2)	(a)	(ウ) 情報システムに関連する脆弱性についての対策要件	対象外	情報システムに関連する脆弱性についての対策要件を策定することは、クラウドサービス利用有無にかかわらず、情報システムセキュリティ責任者が検討すべき事項である。	情報システムに関連する脆弱性についての対策要件を策定することについては、本リファレンスの説明の対象外。	
5	5.2	5.2.1	(2)	(b)	情報システムセキュリティ責任者は、インターネット回線と接続する情報システムを構築する場合は、接続するインターネット回線を定めた上で、標的型攻撃を始めとするインターネットからの様々なサイバー攻撃による情報の漏えい、改ざん等のリスクを低減するための多重防御のためのセキュリティ要件を策定すること。	対象外	インターネット回線と接続する情報システムを構築する場合、接続するインターネット回線を定めた上で、標的型攻撃を始めとするインターネットからの様々なサイバー攻撃による情報の漏えい、改ざん等のリスクを低減するための多重防御のためのセキュリティ要件を策定することは、クラウドサービス利用有無にかかわらず、情報システムセキュリティ責任者が検討すべき事項である。	インターネット回線と接続する情報システムを構築する場合、接続するインターネット回線を定めた上で、標的型攻撃を始めとするインターネットからの様々なサイバー攻撃による情報の漏えい、改ざん等のリスクを低減するための多重防御のためのセキュリティ要件を策定することについては、本リファレンスの説明の対象外。	
					（削除）	対象外	国民・企業と政府との間で申請及び届出等のオンライン手続を提供するシステムについて、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」に基づきセキュリティ要件を策定することは、クラウドサービス利用有無にかかわらず、情報システムセキュリティ責任者が検討すべき事項である。	国民・企業と政府との間で申請及び届出等のオンライン手続を提供するシステムについて、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」に基づきセキュリティ要件を策定することについては、本リファレンスの説明の対象外。	
5	5.2	5.2.1	(2)	(c)	情報システムセキュリティ責任者は、機器等を調達する場合には、「IT 製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定すること。	対象外	機器等を調達する場合、「IT製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定することは、クラウドサービス利用有無にかかわらず、情報システムセキュリティ責任者が検討すべき事項である。	機器等を調達する場合、「IT製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定することについては、本リファレンスの説明の対象外。	
5	5.2	5.2.1	(2)	(d)	情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システム全体の情報セキュリティ水準を低下させることのないように、基盤となる情報システムの情報セキュリティ対策に関する運用管理規程等に基づいたセキュリティ要件を適切に策定すること。	対象外	基盤となる情報システムを利用して情報システムを構築する場合、基盤となる情報システム全体の情報セキュリティ水準を低下させることのないように、基盤となる情報システムの情報セキュリティ対策に関する運用管理規程等に基づいたセキュリティ要件を適切に策定することは、クラウドサービス利用有無にかかわらず、情報システムセキュリティ責任者が検討すべき事項である。	基盤となる情報システムを利用して情報システムを構築する場合、基盤となる情報システム全体の情報セキュリティ水準を低下させることのないように、基盤となる情報システムの情報セキュリティ対策に関する運用管理規程等に基づいたセキュリティ要件を適切に策定することについては、本リファレンスの説明の対象外。	
5	5.2	5.2.1	(3)	情報システムの構築を外部委託する場合の対策					
5	5.2	5.2.1	(3)	(a)	情報システムセキュリティ責任者は、情報システムの構築を外部委託する場合は、以下の事項を含む委託先に実施させる事項を、調達仕様書に記載するなどして、適切に実施させること。	対象外	情報システムの構築を外部委託する場合、委託先に実施させる事項を調達仕様書に記載するなどして適切に実施させることは、クラウドサービス利用有無にかかわらず、情報システムセキュリティ責任者が検討すべき事項である。	情報システムの構築を外部委託する場合、委託先に実施させる事項を調達仕様書に記載するなどして適切に実施させることについては、本リファレンスの説明の対象外。	
5	5.2	5.2.1	(3)	(a)	(ア) 情報システムのセキュリティ要件の適切な実装	対象外	情報システムのセキュリティ要件の適切な実装を実施させることは、クラウドサービス利用有無にかかわらず、情報システムセキュリティ責任者が検討すべき事項である。	情報システムのセキュリティ要件の適切な実装を実施させることについては、本リファレンスの説明の対象外。	
5	5.2	5.2.1	(3)	(a)	(イ) 情報セキュリティの観点に基づく試験の実施	対象外	情報セキュリティの観点に基づく試験を実施させることは、クラウドサービス利用有無にかかわらず、情報システムセキュリティ責任者が検討すべき事項である。	情報セキュリティの観点に基づく試験を実施させることについては、本リファレンスの説明の対象外。	

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
5	5.2	5.2.1	(3)	(a)	(ウ) 情報システムの開発環境及び開発工程における情報セキュリティ対策	対象外	情報システムの開発環境及び開発工程における情報セキュリティ対策を実施させることは、クラウドサービス利用有無にかかわらず、情報システムセキュリティ責任者が検討すべき事項である。	情報システムの開発環境及び開発工程における情報セキュリティ対策を実施させることについては、本リファレンスの説明の対象外。	
5	5.2	5.2.1	(4)		情報システムの運用・保守を外部委託する場合の対策				
5	5.2	5.2.1	(4)	(a)	情報システムセキュリティ責任者は、情報システムの運用・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、調達仕様書に記載するなどして、適切に実施させること。	適合可能	・情報システムセキュリティ責任者は、情報システムの運用・保守を外部委託する場合は、AWSクラウドを利用する場合も、AWSクラウドを利用しない従来の情報システムと同様に、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、調達仕様書に記載するなどして、適切に実施させる必要がある。 [留意事項] ・AWSが取得しているISO27001等の認証で、AWSのセキュリティ機能の運用内容について確認の上、AWSクラウド利用が可能であるか判断する。 ・AWSクラウドを利用する場合は、AWSが自動でセキュリティパッチ適用などの脆弱性対策を行うサービスと利用者が実施する必要があるサービスがあるため留意する。	・AWSは、ISO27001の認定に準拠し、事故対応プログラムを開発し、適切に監視を行っており、利用者は、これらの認証を取得していることを確認可能である。 ・AWSは、ISO27001、NIST、PCI DSSに準拠し、AWS責任範囲においてサービス提供をサポートするシステムにパッチを適用しており、利用者は、これらの認証を取得していることを確認可能である。	・AWS 事故対応プログラム (事故の検出、調査、および対応) は、ISO 27001 基準に合わせて開発されており、システムユーティリティは適切に制限および監視されています。AWS SOC レポートには、システムアクセスを制限するために実施している統制の詳細情報が記載されています。 詳細については、AWS セキュリティプロセスの概要 (http://aws.amazon.com/security で入手可能) を参照してください。 ・AWS 情報システムは、ISO 27001 基準に合わせて、NTP (Network Time Protocol) を介して同期される内部システムクロックを利用しています。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。 AWS は、自動モニタリングシステムを活用して、ハイレベルなサービスパフォーマンスと可用性を提供します。内部的、外部的両方の使用において、様々なオンラインツールを用いた積極的モニタリングが可能です。AWS 内のシステムには膨大な装置が備わっており、主要なオペレーションメトリックをモニタリングしています。 重要計測値が早期警戒しきい値を超える場合に運用管理担当者に自動的に通知されるよう、アラームが設定されています。オンコールスケジュールが採用されているので、担当者が運用上の問題にいつでも対応できます。ポケットベルシステムがサポートされ、アラームが迅速かつ確実に運用担当者に届きます。 詳細については、次のウェブサイトで入手可能な AWS クラウドセキュリティホワイトペーパーを参照してください。http://aws.amazon.com/security。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf AWS は、ハイパーバイザーおよびネットワーキングサービスなど、お客様へのサービス提供をサポートするシステムにパッチを適用する責任を持ちます。この処理は、AWS ポリシーに従い、また ISO 27001、NIST、および PCI の要件に準拠して、必要に応じて実行します。お客様が使用しているゲストオペレーティングシステム、ソフトウェア、およびアプリケーションの統制については、お客様が行い、お客様がそれらのシステムにパッチを適用する責任を持ちます。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf お客様は、自身のゲストオペレーティングシステム、ソフトウェア、アプリケーションの統制を有しており、脆弱性スキャンを実行し、お客様のシステムにパッチを適用するのは、お客様の責任です。対象をお客様のインスタンスに限定し、かつ AWS 利用規約に違反しない限り、お客様はご自身のクラウドインフラストラクチャのスキャンを実施する許可をリクエストできます。AWS セキュリティは、すべてのインターネット向きサービスエンドポイントの IP アドレスの脆弱性を定期的にスキャンしています。判明した脆弱性があれば、修正するために適切な関係者に通知します。通常、AWS の保守およびシステムのパッチ適用はお客様に影響がありません。 詳細については、AWS クラウドセキュリティホワイトペーパーを参照してください (http://aws.amazon.com/security で入手可能)。詳細については、ISO 27001 基準の付録 A、ドメイン 12 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf
5	5.2	5.2.1	(4)	(b)	情報システムセキュリティ責任者は、情報システムの運用・保守を外部委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、速やかに報告させること。	適合可能	・情報システムセキュリティ責任者は、AWSクラウドを利用する場合も、AWSクラウドを利用しない従来の情報システムと同様に、情報システムの運用・保守を外部委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、速やかに報告させることは必要である。 [留意事項] ・AWSによるクラウドプラットフォームの変更 AWSが提供しているAWS クラウドセキュリティ（セキュリティ速報）にてクラウドプラットフォームの変更内容について確認可能である。 ・AWS利用者による情報システムの変更 AWS リソースの設定変更通知について、AWSクラウドの提供する機能(AWS Config)を利用することが望ましい。	・AWSクラウドではクラウドプラットフォームに対する変更がある場合、AWS クラウドセキュリティ（セキュリティ速報）にて当該内容が記録され、利用者は変更内容を確認可能である。 ・AWSクラウドは、AWS Configサービスにて、AWS リソースインベントリ、設定履歴、および設定変更通知といった機能を提供する。また、既存のAWS リソースと削除された AWS リソースとの検出、ルールに対する全体的なコンプライアンスの判定、および任意の時点でのリソース設定の詳細な調査が可能。	・アマゾン ウェブ サービスは現在、Service Organization Controls 1 (SOC 1)、Type II レポートを発行しています。レポートには AWS SOC 1 の統制目標が記載されており、このレポート自体に、各統制目標と独立監査人による各統制のテスト手順の結果をサポートする統制活動が特定されています。 変更管理 ・統制は、既存の IT リソースに対する変更 (緊急/特殊な設定) が記録され、認証され、試験され、承認されて文書化されることについて、合理的な保証を提供するものです。 詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf ソフトウェア AWS は、変更の管理にシステム的なアプローチを採用しています。そのためお客様に影響を与えるサービスの変更は、徹底的に検証、テスト、承認され、充分な情報が提供されます。AWS の変更管理プロセスは、意図しないサービス障害を防ぎ、お客様に対するサービスの完全性を維持することを目的としています。実稼働環境にデプロイされる変更には、以下の対応が行われます: • 検証: 変更の技術的側面について専門家による検証が必要です。 • テスト: 適用されている変更は、予想どおりに動作し、パフォーマンスに悪影響を与えないことを確認するためにテストされます。 • 承認: すべての変更は、ビジネスへの影響を適切に監視し、それらの影響についての情報を提供するために、承認される必要があります。 詳細に関しては「セキュリティプロセスの概要（2014年11月）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf AWS Config は完全マネージド型のサービスで、セキュリティとガバナンスのため、AWS リソースインベントリ、設定履歴、および設定変更通知といった機能が用意されています。Config Rules を使用して、AWS Config によって記録された AWS リソース設定を自動的にチェックするルールを作成できます。 AWS Config を使用することで、既存の AWS リソースと削除された AWS リソースとの検出、ルールに対する全体的なコンプライアンスの判定、および任意の時点でのリソース設定の詳細な調査が可能になります。これらの機能は、コンプライアンス監査、セキュリティ分析、リソース変更の追跡、トラブルシューティングを可能にします。 詳細に関しては、https://aws.amazon.com/jp/config/ を参照してください。 AWS クラウドセキュリティ（セキュリティ速報） No matter how carefully engineered the services are, from time to time it may be necessary to notify customers of security and privacy events with AWS services. We will publish security bulletins. 詳細に関しては、 https://aws.amazon.com/jp/security/security-bulletins/ を参照してください。
5	5.2	5.2.2	(1)		機器等の選定時の対策				
5	5.2	5.2.2	(1)	(a)	情報システムセキュリティ責任者は、機器等の選定時において、選定基準に対する機器等の適合性を確認し、その結果を機器等の選定における判断の一要素として活用すること。	対象外			
5	5.2	5.2.2	(2)		情報システムの構築時の対策				
5	5.2	5.2.2	(2)	(a)	情報システムセキュリティ責任者は、情報システムの構築において、情報セキュリティの観点から必要な措置を講ずること。	対象外			
5	5.2	5.2.2	(2)	(b)	情報システムセキュリティ責任者は、構築した情報システムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講ずること。	対象外			
5	5.2	5.2.2	(3)		納品検査時の対策				

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
5	5.2	5.2.2	(3)	(a)	情報システムセキュリティ責任者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認すること。	対象外			
5	5.2	5.2.2	(3)	(b)	情報システムセキュリティ責任者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認すること。	対象外			
5	5.2	5.2.3	情報システムの運用・保守						
5	5.2	5.2.3	(1)	情報システムの運用・保守時の対策					
5	5.2	5.2.3	(1)	(a)	情報システムセキュリティ責任者は、情報システムの運用・保守において、情報システムに実装されたセキュリティ機能を適切に運用すること。	対象外			
5	5.2	5.2.3	(1)	(b)	情報システムセキュリティ責任者は、基盤となる情報システムを利用して構築された情報システムを運用する場合は、基盤となる情報システムを整備し運用管理する機関等との責任分界に応じた運用管理体制の下、基盤となる情報システムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切に情報システムを運用すること。	対象外			
5	5.2	5.2.3	(1)	(c)	情報システムセキュリティ責任者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理すること。	対象外			
5	5.2	5.2.4	情報システムの更改・廃棄						
5	5.2	5.2.4	(1)	情報システムの更改・廃棄時の対策					
5	5.2	5.2.4	(1)	(a)	情報システムセキュリティ責任者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下の措置を適切に講ずること。	対象外			
5	5.2	5.2.4	(1)	(a)	(ア) 情報システム更改時の情報の移行作業における情報セキュリティ対策	対象外	情報システム更改時の情報の移行作業における情報セキュリティ対策を講じることは、クラウドサービス利用有無にかかわらず、情報システムセキュリティ責任者が遵守すべき事項である。	情報システム更改時の情報の移行作業における情報セキュリティ対策を講じることについては、本リファレンスの説明の対象外。	

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
5	5.2	5.2.4	(1)	(a)	(イ) 情報システム廃棄時の不要な情報の抹消	適合可能	・情報システムを廃棄する場合には、AWSクラウドを利用する場合も、AWSクラウドを利用しない従来の情報システムと同様に、不要な情報が残らないように抹消する必要がある。 [留意事項] ・AWSクラウド上のデータ管理に関しては、提供される暗号化機能やサービスを利用した暗号化を実施し、システム利用終了時に暗号鍵そのものを廃棄することで、データ抹消に相当するといった対応を考慮することも可能である。	・AWSクラウドは、ストレージデバイスが製品寿命に達した場合、ISO27001の基準に準拠し廃棄を行っており、利用者はAWS ISO27001認定証によりAWSの実施内容を検証することが可能である。 ・削除した EBS ボリュームが使用していた物理的なブロックストレージは、別のアカウントに割り当てられる前に、ゼロで上書きされる。	AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M (国家産業セキュリティプログラム運営マニュアル) または NIST 800-88 (媒体のサニタイズに関するガイドライン) に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。詳細については、次のウェブサイトで入手可能な AWS クラウドセキュリティホワイトペーパーを参照してください。 http://aws.amazon.com/security/。 Amazon EBS ボリュームは、ワイプ処理を行った後、未フォーマットのロープロックデバイスとしてお客様に提供されます。ワイプは再使用の直前に実施されるため、お客様に提供された時点でワイプ処理は完了しています。業務手順上、DoD 5220.22-M (「国家産業セキュリティプログラム運営マニュアル」) や NIST 800-88 (「媒体のサニタイズに関するガイドライン」) が指定するような、特定の方法で全データをワイプする必要がある場合、お客様自身で Amazon EBS のワイプ作業を行うこともできます。お客様がしかるべき手順でワイプを実施してからボリュームを削除することで、コンプライアンスの要件を満たすようにします。 機密データの暗号化は、一般的なセキュリティのベストプラクティスです。AWS には、EBS ボリュームとスナップショットを AES-256 で暗号化する機能があります。EC2 インスタンスをホストするサーバーで暗号化が行われるため、EC2 インスタンスと EBS ストレージとの間を移動するデータが暗号化されます。この処理が効率的に低レイテンシーで行われるようにするために、EBS 暗号化機能は EC2 の強力なインスタンスタイプ (たとえば、M3、C3、R3、G2) だけで使用できます。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf ISO 27001 基準に合わせて、AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M (国家産業セキュリティプログラム運営マニュアル) または NIST 800-88 (媒体のサニタイズに関するガイドライン) に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。 詳細については、ISO 27001 基準の付録 A、ドメイン 8 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf EBS ボリュームは、インスタンスの運用状況に左右されない永続性のあるストレージを提供します。データが維持される限り、ボリュームの使用料が発生します。 デフォルトでは、実行中のインスタンスにアタッチされている EBS ボリュームは、データはそのままの状態で、インスタンスが終了すると自動的にインスタンスからデタッチされます。デタッチされたボリュームは新しいインスタンスに再アタッチできるので、迅速な復旧が可能です。EBS-backed インスタンスを使用している場合は、アタッチしたボリュームに格納されているデータに影響を与えることなく、インスタンスを停止および再起動できます。ボリュームは停止/起動のサイクルを通じてアタッチされたままです。これにより、必要なときに処理リソースとストレージリソースを使用するだけで、ボリュームでのデータの処理と格納を永続的に実行できるようになります。データは、ボリュームを明示的に削除するまでボリュームに保持されます。削除した EBS ボリュームが使用していた物理的なブロックストレージは、別のアカウントに割り当てられる前に、ゼロで上書きされます。機密データを扱っている場合は、手動によるデータの暗号化や、Amazon EBS 暗号化 で保護されているボリュームへのデータの格納を検討してください。詳細については、「Amazon EBS Encryption」を参照してください。 デフォルトでは、インスタンスの起動時に作成およびアタッチされた EBS ボリュームは、インスタンスの終了時に削除されます。この動作を変更するには、インスタンスの起動時にフラグ DeleteOnTermination の値を false に変更します。値を変更すると、インスタンスが終了してもボリュームが保持されるので、そのボリュームを別のインスタンスにアタッチできます。 詳細に関してはhttp://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSVolumes.htmlをご参照下さい。
5	5.2	5.2.5	情報システムについての対策の見直し						
5	5.2	5.2.5	(1)	情報システムについての対策の見直し					
5	5.2	5.2.5	(1)	(a)	情報システムセキュリティ責任者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずること。	適合可能	・情報システムセキュリティ責任者は、AWSクラウドを利用する場合も、AWSクラウドを利用しない従来の情報システムと同様に、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずる必要がある。 [留意事項] ・AWSクラウドを利用する場合は、AWSクラウドの責任範囲を確認し、対象外の範囲については情報システムセキュリティ責任者が対策を行う必要があることに留意する。 ・AWSが取得しているISO27001等の認証で、AWSの情報セキュリティ対策として新たな脅威の出現、運用、監視等の状況により見直しを適時実施されているかを確認の上、AWSクラウド利用が可能であるか判断する。	・AWSは、ISO 27001の認定に準拠し、情報セキュリティリスクを管理する継続的なアプローチを行っており、利用者は、これらの認証を取得していることを確認可能である。	AWS は、ISO 27001 に合わせて、リスク管理プログラムを維持してリスクを軽減し、管理しています。 AWS マネジメントには、リスクを緩和または管理するためのリスク特定やコントロールの実装など、戦略的事業計画があります。また、少なくとも半年に一度、戦略的事業計画を再評価します。このプロセスでは、マネジメントがその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。 AWS のリスク管理プログラムは、PCI DSS、ISO 27001、および FedRAMP への準拠のため、監査中に外部の独立監査人によって確認されます。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf ISO 27001/27002 は世界で広く採用されているセキュリティ基準で、会社とカスタマー情報の管理の体系的なアプローチの要件とベストプラクティスを定めるものです。これは、刻々と変化する脅威のシナリオに適する定期的リスク査定に基づいています。認定を取得するためには、会社とカスタマー情報の機密性、完全性、および可用性に影響を与える情報セキュリティリスクを管理する体系的かつ継続的なアプローチが会社にあることを示す必要があります。この認定は、セキュリティ管理や作業に関する重要情報を提供するという Amazon の取り組みを補強するものです。 詳細に関しては「リスクおよびコンプライアンス（2015年12月）」をご参照下さい。 https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf
5	5.3	情報システムの運用継続計画							
5	5.3	5.3.1	情報システムの運用継続計画の整備・整合的運用の確保						
5	5.3	5.3.1	(1)	情報システムの運用継続計画の整備・整合的運用の確保					
5	5.3	5.3.1	(1)	(a)	統括情報セキュリティ責任者は、機関等において非常時優先業務を支える情報システムの運用継続計画を整備する必要がある場合は、非常時における情報セキュリティに係る対策事項を検討すること。	対象外			
5	5.3	5.3.1	(1)	(b)	統括情報セキュリティ責任者は、情報システムの運用継続計画の教育訓練や維持改善を行う際等に、非常時における情報セキュリティに係る対策事項が運用可能であるかを確認すること。	対象外			
6	6.1	情報システムのセキュリティ要件							
6	6.1	6.1.1	主体認証機能						
6	6.1	6.1.1	(1)	主体認証機能の導入					

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
6	6.1	6.1.1	(1)	(a)	情報システムセキュリティ責任者は、情報システムや情報へのアクセス主体を特定し、それが正当な主体であることを検証する必要がある場合、主体の識別及び主体認証を行う機能を設けること。	適合可能	・情報システムセキュリティ責任者は、情報システム（業務アプリケーション）に主体認証機能を設けるにあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド上に独自に構築するアプリケーションへのアクセスコントロールは、情報システムセキュリティ責任者が機能を設ける必要があることに留意する。 ・AWSクラウドを利用する場合、AWSクラウド上の割り当て領域に運用管理上アクセスする者の認証に AWS IAMを利用することに留意する。 ・認証機能とアプリケーションの設置場所（例：認証はオンプレミス、アプリケーションはクラウド）によっては、利用できるテクノロジーに制約があったり、Internetを介した認証データの受け渡しに性能上の制約が出る場合があることに留意する。	・AWSクラウドは、IAM及びMFAの機能を提供しており、当該機能を用いることで、利用者のAWSリソースへのアクセスのコントロール（主体の識別及び主体認証を含む）が可能である。 ・AWSはISO 27001、PCI、ITAR、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（主体の識別及び主体認証含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（主体の識別及び主体認証含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	AWS Identity and Access Management(IAM)により、お客様のユーザーのAWSサービスおよびリソースへのアクセスを安全にコントロールすることができます。IAMを使用すると、AWSのユーザーとグループを作成および管理し、アクセス権を使用してAWSリソースへのアクセスを許可および拒否できます。詳細に関しては、https://aws.amazon.com/jp/iam/ を参照してください。 AWS Multi-Factor Authentication(MFA)は、ユーザー名とパスワードに加えて保護を強化できる、簡単なベストプラクティスです。MFAを有効にすると、ユーザーがAWSウェブサイトにサインインするときに、ユーザー名とパスワードの他に、AWS MFAデバイスからの認証コードを入力することが必要になります。このように複数の要素を組み合わせることによって、AWSアカウントの設定とリソースのセキュリティが強化されます。詳細に関しては、https://aws.amazon.com/jp/iam/details/mfa/を参照してください。 所定の統制によってシステムおよびデータのアクセスを制限し、AWSアクセスポリシーに従ってシステムまたはデータに対するアクセスを制限および監視できるようにしています。さらに、お客様のデータおよびサーバーインスタンスは、デフォルトで他のお客様とは論理的に隔離されています。特権のあるユーザーアクセス制御は、AWS SOC、ISO 27001、PCI、ITAR、およびFedRAMPの監査中に独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf
6	6.1	6.1.1	(1)	(b)	情報システムセキュリティ責任者は、国民・企業と機関等との間の申請、届出等のオンライン手続を提供する情報システムを構築する場合は、オンライン手続におけるリスクを評価した上で、主体認証に係る要件を策定すること。	対象外	国民・企業と機関等との間でオンライン手続を提供する情報システムを構築する場合は、クラウドサービス利用有無にかかわらず、情報システムセキュリティ責任者が検討すべき事項である。	国民・企業と機関等との間でオンライン手続を提供する情報システムを構築する場合については、本リファレンスの説明の対象外。	
6	6.1	6.1.1	(1)	(c)	情報システムセキュリティ責任者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずること。	適合可能	・情報システムセキュリティ責任者は、情報システム（業務アプリケーション）において、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずるにあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド上に独自に構築するアプリケーションへのアクセスコントロールは、情報システムセキュリティ責任者が機能を設ける必要があることに留意する。 ・AWSクラウドを利用する場合、AWSクラウド上の割り当て領域に運用管理上アクセスする者の認証に AWS IAMを利用するが、この AWS IAM の設定・運用についても、本項が求める要件を満たす必要があることに留意する。特に、府省庁対策ガイドラインの基本的対策事項については、AWS提供の機能に加え、官公庁の情報システムの運用対処が必要となる事項もあるため、これらを踏まえた検討（設計、構築、運用等）を行う必要があることに留意する。 ・AWS IAMにおいてパスワードが失効した場合でもアクセスキーにより一部操作が可能であるため、アクセスキー無効化等の運用措置が必要となることに留意する。	・AWSクラウドは、IAM及びMFAの機能を提供しており、当該機能を用いることで、利用者のAWSリソースへのアクセスのコントロール（不正行為及び不正な主体認証の試行への対抗を含む）が可能である。 ・AWSクラウドは、AWS CloudTrail及びAWS CloudWatchを提供しており、当該機能を用いることで、利用者のAWSリソースについて、正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログの取得が可能である。 ・AWSはISO 27001、PCI、ITAR、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（不正行為及び不正な主体認証の試行への対抗を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（不正行為及び不正な主体認証の試行への対抗を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	AWS Identity and Access Management(IAM)により、お客様のユーザーのAWSサービスおよびリソースへのアクセスを安全にコントロールすることができます。IAMを使用すると、AWSのユーザーとグループを作成および管理し、アクセス権を使用してAWSリソースへのアクセスを許可および拒否できます。詳細に関しては、https://aws.amazon.com/jp/iam/ を参照してください。 AWS Multi-Factor Authentication(MFA)は、ユーザー名とパスワードに加えて保護を強化できる、簡単なベストプラクティスです。MFAを有効にすると、ユーザーがAWSウェブサイトにサインインするときに、ユーザー名とパスワードの他に、AWS MFAデバイスからの認証コードを入力することが必要になります。このように複数の要素を組み合わせることによって、AWSアカウントの設定とリソースのセキュリティが強化されます。詳細に関しては、https://aws.amazon.com/jp/iam/details/mfa/を参照してください。 AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。 CloudTrail を使用すると、AWS インフラストラクチャ全体で API 呼び出しに関連するイベントをログに記録し、継続的に監視し、保持できます。詳細に関しては、https://aws.amazon.com/jp/cloudtrail/を参照してください。 Amazon CloudWatch は、AWS クラウドリソースと AWS で実行するアプリケーションのモニタリングサービスです。Amazon CloudWatch を使用して、メトリックスを収集して追跡すること、ログファイルを収集してモニタリングすること、アラームを設定すること、および AWS リソースの変更に自動的に反応することができます。詳細に関しては、https://aws.amazon.com/jp/cloudwatch/を参照してください。 所定の統制によってシステムおよびデータのアクセスを制限し、AWSアクセスポリシーに従ってシステムまたはデータに対するアクセスを制限および監視できるようにしています。さらに、お客様のデータおよびサーバーインスタンスは、デフォルトで他のお客様とは論理的に隔離されています。特権のあるユーザーアクセス制御は、AWS SOC、ISO 27001、PCI、ITAR、およびFedRAMPの監査中に独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf
6	6.1	6.1.1	(2)	識別コード及び主体認証情報の管理					
6	6.1	6.1.1	(2)	(a)	情報システムセキュリティ責任者は、情報システムにアクセスする全ての主体に対して、識別コード及び主体認証情報を適切に付与し、管理するための措置を講ずること。	適合可能	・情報システムセキュリティ責任者は、情報システム（業務アプリケーション）にアクセスする全ての主体に対して、識別コード及び主体認証情報を適切に付与し、管理するための措置を講ずるにあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド上に独自に構築するアプリケーションへのアクセスコントロールは、情報システムセキュリティ責任者が機能を設ける必要があることに留意する。 ・AWSクラウドの割り当て領域に対して運用管理上アクセスする者を識別する認証（AWS IAM等）においても、本項が求める措置を講ずる必要があることに留意する。	・AWSクラウドは、IAM及びMFAの機能を提供しており、当該機能を用いることで、利用者のAWSリソースへのアクセスのコントロール（識別コード及び主体認証情報の付与・管理を含む）が可能である。 ・AWSはISO 27001、PCI、ITAR、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（識別コード及び主体認証情報の付与・管理）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（識別コード及び主体認証情報の付与・管理）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	AWS Identity and Access Management(IAM)により、お客様のユーザーのAWSサービスおよびリソースへのアクセスを安全にコントロールすることができます。IAMを使用すると、AWSのユーザーとグループを作成および管理し、アクセス権を使用してAWSリソースへのアクセスを許可および拒否できます。詳細に関しては、https://aws.amazon.com/jp/iam/ を参照してください。 AWS Multi-Factor Authentication(MFA)は、ユーザー名とパスワードに加えて保護を強化できる、簡単なベストプラクティスです。MFAを有効にすると、ユーザーがAWSウェブサイトにサインインするときに、ユーザー名とパスワードの他に、AWS MFAデバイスからの認証コードを入力することが必要になります。このように複数の要素を組み合わせることによって、AWSアカウントの設定とリソースのセキュリティが強化されます。詳細に関しては、https://aws.amazon.com/jp/iam/details/mfa/を参照してください。 所定の統制によってシステムおよびデータのアクセスを制限し、AWSアクセスポリシーに従ってシステムまたはデータに対するアクセスを制限および監視できるようにしています。さらに、お客様のデータおよびサーバーインスタンスは、デフォルトで他のお客様とは論理的に隔離されています。特権のあるユーザーアクセス制御は、AWS SOC、ISO 27001、PCI、ITAR、およびFedRAMPの監査中に独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
6	6.1	6.1.1	(2)	(b)	情報システムセキュリティ責任者は、主体が情報システムを利用する必要がなくなった場合は、当該主体の識別コード及び主体認証情報の不正な利用を防止するための措置を速やかに講ずること。	適合可能	・情報システムセキュリティ責任者は、主体が情報システム（業務アプリケーション）を利用する必要がなくなった場合に、当該主体の識別コード及び主体認証情報の不正な利用を防止するための措置を速やかに講ずるにあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド上に独自に構築するアプリケーションへのアクセスコントロールは、情報システムセキュリティ責任者が機能を設ける必要があることに留意する。 ・AWSクラウドの割り当て領域に対して運用管理上アクセスする者が、運用業務を離れるなどの理由で利用する必要がなくなった場合についても、本項が求める措置を講ずる必要があることに留意する。	・AWSクラウドは、IAM及びMFAの機能を提供しており、当該機能を用いることで、利用者のAWSリソースへのアクセスのコントロール（アクセス主体の識別コード及び主体認証情報の不正利用防止を含む）が可能である。 ・AWSクラウドは、AWS CloudTrail及びAWS CloudWatchを提供しており、当該機能を用いることで、利用者のAWSリソースについて、正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログの取得が可能である。 ・AWSはISO 27001、PCI、ITAR、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（アクセス主体の識別コード及び主体認証情報の不正利用防止を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（アクセス主体の識別コード及び主体認証情報の不正利用防止を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	AWS Identity and Access Management(IAM)により、お客様のユーザーのAWSサービスおよびリソースへのアクセスを安全にコントロールすることができます。IAMを使用すると、AWSのユーザーとグループを作成および管理し、アクセス権を使用してAWSリソースへのアクセスを許可および拒否できます。詳細に関しては、https://aws.amazon.com/jp/iam/ を参照してください。 AWS Multi-Factor Authentication(MFA)は、ユーザー名とパスワードに加えて保護を強化できる、簡単なベストプラクティスです。MFAを有効にすると、ユーザーがAWSウェブサイトにサインインするときに、ユーザー名とパスワードの他に、AWS MFAデバイスからの認証コードを入力することが必要になります。このように複数の要素を組み合わせることによって、AWSアカウントの設定とリソースのセキュリティが強化されます。詳細に関しては、https://aws.amazon.com/jp/iam/details/mfa/を参照してください。 AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。 CloudTrail を使用すると、AWS インフラストラクチャ全体で API 呼び出しに関連するイベントをログに記録し、継続的に監視し、保持できます。詳細に関しては、https://aws.amazon.com/jp/cloudtrail/を参照してください。 Amazon CloudWatch は、AWS クラウドリソースと AWS で実行するアプリケーションのモニタリングサービスです。Amazon CloudWatch を使用して、メトリックスを収集して追跡すること、ログファイルを収集してモニタリングすること、アラームを設定すること、および AWS リソースの変更に自動的に反応することができます。詳細に関しては、https://aws.amazon.com/jp/cloudwatch/を参照してください。 所定の統制によってシステムおよびデータのアクセスを制限し、AWSアクセスポリシーに従ってシステムまたはデータに対するアクセスを制限および監視できるようにしています。さらに、お客様のデータおよびサーバーインスタンスは、デフォルトで他のお客様とは論理的に隔離されています。特権のあるユーザーアクセス制御は、AWS SOC、ISO 27001、PCI、ITAR、およびFedRAMPの監査中に独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf
6	6.1	6.1.2	アクセス制御機能						
6	6.1	6.1.2	(1)	アクセス制御機能の導入					
6	6.1	6.1.2	(1)	(a)	情報システムセキュリティ責任者は、情報システムの特性、情報システムが取り扱う情報の格付及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設けること。	適合可能	・情報システムセキュリティ責任者は、情報システム（業務アプリケーション）の特性、情報システムが取り扱う情報の格付及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設けるにあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド上に独自に構築するアプリケーションへのアクセスコントロールは、情報システムセキュリティ責任者が機能を設ける必要があることに留意する。 ・AWSクラウドの割り当て領域に対するアクセス制御機能（AWS IAM等を利用）についても、本項が求める機能を設ける必要があることに留意する。 ・IPアドレスによる端末の制限は、Amazon EC2 の管理者アカウントに対しても設定可能であることを考慮の上、アクセス制御を設計することが望ましい。 ・AWSクラウドを利用する場合、AWSクラウドへの管理者としてのアクセスと、一般ユーザとしてのアクセスにおいて、同じIPアドレスを使うことになるが、AWS IAM セキュリティグループを適切に設定することによって、AWSクラウドの管理用機能を管理者のみに限定できることを考慮の上、アクセス制御を設計することが望ましい。	・AWSクラウドは、IAMの機能を提供しており、当該機能を用いることで、利用者のAWSリソースへのアクセスのコントロール（権限を有する者のみがアクセス制御設定できる措置を含む）が可能である。 ・AWSはISO 27001、PCI、ITAR、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（権限を有する者のみがアクセス制御設定できる措置を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSクラウドの基盤部分の運用（権限を有する者のみがアクセス制御設定できる措置を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	AWS Identity and Access Management(IAM)により、お客様のユーザーのAWSサービスおよびリソースへのアクセスを安全にコントロールすることができます。IAMを使用すると、AWSのユーザーとグループを作成および管理し、アクセス権を使用してAWSリソースへのアクセスを許可および拒否できます。詳細に関しては、https://aws.amazon.com/jp/iam/ を参照してください。 所定の統制によってシステムおよびデータのアクセスを制限し、AWSアクセスポリシーに従ってシステムまたはデータに対するアクセスを制限および監視できるようにしています。さらに、お客様のデータおよびサーバーインスタンスは、デフォルトで他のお客様とは論理的に隔離されています。特権のあるユーザーアクセス制御は、AWS SOC、ISO 27001、PCI、ITAR、およびFedRAMPの監査中に独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf
6	6.1	6.1.2	(1)	(b)	情報システムセキュリティ責任者は、情報システム及び情報へのアクセスを許可する主体が確実に制限されるように、アクセス制御機能を適切に運用すること。	適合可能	・情報システムセキュリティ責任者は、情報システム（業務アプリケーション）における適切なアクセス制御の運用について、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド上に独自に構築するアプリケーションへのアクセスコントロールは、情報システムセキュリティ責任者が機能を設ける必要があることに留意する。 ・AWSクラウドの割り当て領域に対するアクセス制御機能（AWS IAM等を利用）を用いて、どのようにアクセス制御を運用するのかについても、政府統一基準の本項が求める運用を行う必要があることに留意する。	・AWSクラウドは、IAMの機能を提供しており、当該機能を用いることで、利用者のAWSリソースへのアクセスのコントロール（アクセス制御の適切な運用を含む）が可能である。 ・AWSクラウドは、AWS CloudTrail及びAWS CloudWatchを提供しており、当該機能を用いることで、利用者のAWSリソースについて、正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログの取得が可能である。 ・AWSはISO 27001、PCI、ITAR、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（アクセス制御の適切な運用を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（アクセス制御の適切な運用を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	AWS Identity and Access Management(IAM)により、お客様のユーザーのAWSサービスおよびリソースへのアクセスを安全にコントロールすることができます。IAMを使用すると、AWSのユーザーとグループを作成および管理し、アクセス権を使用してAWSリソースへのアクセスを許可および拒否できます。詳細に関しては、https://aws.amazon.com/jp/iam/ を参照してください。 AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。 CloudTrail を使用すると、AWS インフラストラクチャ全体で API 呼び出しに関連するイベントをログに記録し、継続的に監視し、保持できます。詳細に関しては、https://aws.amazon.com/jp/cloudtrail/を参照してください。 Amazon CloudWatch は、AWS クラウドリソースと AWS で実行するアプリケーションのモニタリングサービスです。Amazon CloudWatch を使用して、メトリックスを収集して追跡すること、ログファイルを収集してモニタリングすること、アラームを設定すること、および AWS リソースの変更に自動的に反応することができます。詳細に関しては、https://aws.amazon.com/jp/cloudwatch/を参照してください。 所定の統制によってシステムおよびデータのアクセスを制限し、AWSアクセスポリシーに従ってシステムまたはデータに対するアクセスを制限および監視できるようにしています。さらに、お客様のデータおよびサーバーインスタンスは、デフォルトで他のお客様とは論理的に隔離されています。特権のあるユーザーアクセス制御は、AWS SOC、ISO 27001、PCI、ITAR、およびFedRAMPの監査中に独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf
6	6.1	6.1.3	権限の管理						
6	6.1	6.1.3	(1)	権限の管理					

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
6	6.1	6.1.3	(1)	(a)	情報システムセキュリティ責任者は、主体から対象に対するアクセスの権限を適切に設定するよう、措置を講ずること。	適合可能	・情報システムセキュリティ責任者は、情報システム（業務アプリケーション）における主体から対象に対するアクセスの権限を適切に設定するための措置について、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド上に独自に構築するアプリケーションへのアクセスコントロールは、情報システムセキュリティ責任者が機能を設ける必要があることに留意する。 ・AWSクラウドの割り当て領域に対する運用管理上のアクセス権限の設定（AWS IAM等を利用）についても、本項が求める措置を講ずる必要があることに留意する。	・AWSクラウドは、IAMの機能を提供しており、当該機能を用いることで、利用者のAWSリソースへのアクセスのコントロール（アクセス制御の適切な設定のための措置を含む）が可能である。 ・AWSはISO 27001、PCI、ITAR、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（アクセス制御の適切な設定のための措置を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（アクセス制御の適切な設定のための措置を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	AWS Identity and Access Management(IAM)により、お客様のユーザーのAWSサービスおよびリソースへのアクセスを安全にコントロールすることができます。IAMを使用すると、AWSのユーザーとグループを作成および管理し、アクセス権を使用してAWSリソースへのアクセスを許可および拒否できます。詳細に関しては、https://aws.amazon.com/jp/iam/ を参照してください。 所定の統制によってシステムおよびデータのアクセスを制限し、AWSアクセスポリシーに従ってシステムまたはデータに対するアクセスを制限および監視できるようにしています。さらに、お客様のデータおよびサーバーインスタンスは、デフォルトで他のお客様とは論理的に隔離されています。特権のあるユーザーアクセス制御は、AWS SOC、ISO 27001、PCI、ITAR、およびFedRAMPの監査中に独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf
6	6.1	6.1.3	(1)	(b)	情報システムセキュリティ責任者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講ずること。	適合可能	・情報システムセキュリティ責任者は、情報システム（業務アプリケーション）において、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置について、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド上に独自に構築するアプリケーションへのアクセスコントロールは、情報システムセキュリティ責任者が機能を設ける必要があることに留意する。 ・AWSクラウドの割り当て領域にアクセスできる管理者権限についても、本項が求める措置を講ずる必要があることに留意する。 ・AWSクラウドの割り当て領域における管理者権限の特権を持つユーザについては、AWS クラウドの提供する AWS IAM にて管理する必要があることに留意する。	・AWSクラウドは、IAMの機能を提供しており、当該機能を用いることで、利用者のAWSリソースへのアクセスのコントロール（管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を含む）が可能である。 ・AWSクラウドは、AWS CloudTrail及びAWS CloudWatchを提供しており、当該機能を用いることで、利用者のAWSリソースについて、正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログの取得が可能である。 ・AWSはISO 27001、PCI、ITAR、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	AWS Identity and Access Management(IAM)により、お客様のユーザーのAWSサービスおよびリソースへのアクセスを安全にコントロールすることができます。IAMを使用すると、AWSのユーザーとグループを作成および管理し、アクセス権を使用してAWSリソースへのアクセスを許可および拒否できます。詳細に関しては、https://aws.amazon.com/jp/iam/ を参照してください。 AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。 CloudTrail を使用すると、AWS インフラストラクチャ全体で API 呼び出しに関連するイベントをログに記録し、継続的に監視し、保持できます。詳細に関しては、https://aws.amazon.com/jp/cloudtrail/を参照してください。 Amazon CloudWatch は、AWS クラウドリソースと AWS で実行するアプリケーションのモニタリングサービスです。Amazon CloudWatch を使用して、メトリックスを収集して追跡すること、ログファイルを収集してモニタリングすること、アラームを設定すること、および AWS リソースの変更に自動的に反応することができます。詳細に関しては、https://aws.amazon.com/jp/cloudwatch/を参照してください。 所定の統制によってシステムおよびデータのアクセスを制限し、AWSアクセスポリシーに従ってシステムまたはデータに対するアクセスを制限および監視できるようにしています。さらに、お客様のデータおよびサーバーインスタンスは、デフォルトで他のお客様とは論理的に隔離されています。特権のあるユーザーアクセス制御は、AWS SOC、ISO 27001、PCI、ITAR、およびFedRAMPの監査中に独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf
6	6.1	6.1.4	ログの取得・管理						
6	6.1	6.1.4	(1)	ログの取得・管理					
6	6.1	6.1.4	(1)	(a)	情報システムセキュリティ責任者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得すること。	適合可能	・情報システムセキュリティ責任者は、情報システム（業務アプリケーション）が正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得することについて、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウドが提供するログ関連サービス(CloudTrail, CloudWatch Lサービス等)のみで当該の情報システムに必要なログが全て取得されるとは限らないことに考慮した上で、ログ取得を設計する必要があることに留意する。 ・AWSクラウドを利用する場合には、AWSクラウドが提供するログと、AWSクラウド上に独自に構築するアプリケーションで取得するログを組み合せたログ構成となることに留意する。	・AWSクラウドは、AWS CloudTrail及びAWS CloudWatchを提供しており、当該機能を用いることで、利用者のAWSリソースについて、正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログの取得が可能である。 ・AWSはPCI DSS、ISO 27001、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログの取得を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログの取得を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。 CloudTrail を使用すると、AWS インフラストラクチャ全体で API 呼び出しに関連するイベントをログに記録し、継続的に監視し、保持できます。詳細に関しては、https://aws.amazon.com/jp/cloudtrail/を参照してください。 Amazon CloudWatch は、AWS クラウドリソースと AWS で実行するアプリケーションのモニタリングサービスです。Amazon CloudWatch を使用して、メトリックスを収集して追跡すること、ログファイルを収集してモニタリングすること、アラームを設定すること、および AWS リソースの変更に自動的に反応することができます。詳細に関しては、https://aws.amazon.com/jp/cloudwatch/を参照してください。 AWSはAWSシステム内でシステムとデバイス間で監査可能なイベントカテゴリを識別しています。サービスチームは監査機能を設定して、要件に従って継続的にセキュリティ関連イベントを記録しています。ログストレージシステムは、ログストレージの次のニーズが発生すると自動的に容量を増やす、スケーラブルで高可用性のサービスを提供するように設計されています。AWS内のシステムは、主要な運用メトリックスやセキュリティメトリックスをモニタリングするよう広範に実装されます。重要計測値が早期警戒しきい値を超える場合に運用管理担当者に自動的に通知されるよう、アラームが設定されています。しきい値を超えると、AWSインシデント対応プロセスが開始されます。Amazonインシデント対応チームは、業界標準の診断手順を採用して、ビジネスに影響するイベントに解決策を実行します。スタッフは24時間年中無休でインシデントの検出、影響の管理、および解決にあたっています。 AWSの役割と責任は、SOC、PCI DSS、ISO 27001、およびFedRAMPへの準拠のため、監査中に外部の独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
6	6.1	6.1.4	(1)	(b)	情報システムセキュリティ責任者は、情報システムにおいて、その特性に応じてログを取得する目的を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法、及びログが取得できなくなった場合の対処方法等について定め、適切にログを管理すること。	適合可能	・情報システムセキュリティ責任者は、情報システム（業務アプリケーション）において、その特性に応じてログを取得する目的を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法、及びログが取得できなくなった場合の対処方法等について定め、適切にログを管理することについて、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウドの割り当て領域に対する不正侵入、不正操作等がなされていないことの検証を行うためのログについても管理の対象となるが、AWSが提供するログに関するサービス(CloudTrail, CloudWatchサービス等)の仕様上の理由等により、統一基準が求めるログ管理にかかる項目が一部制約される可能性があることに留意する。 ・ログの保管場所をAWSクラウド以外の場所にする場合には、AWSが提供するログに関するサービス(CloudTrail, CloudWatchサービス等)から、必要なログを適切な頻度でコピーするなどの検討が別途必要になることに留意する。 ・AWSクラウドを利用する場合には、AWSクラウドが提供するログと、AWSクラウド上に独自に構築するアプリケーションで取得するログを組み合せたログ構成となることに留意する。	・AWSクラウドは、AWS CloudTrail及びAWS CloudWatchサービスを提供しており、当該機能を用いることで、利用者のAWSリソースについて、適切なログの管理が可能である。 ・AWSはPCI DSS、ISO 27001、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（適切なログの管理を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（適切なログの管理を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。 CloudTrail を使用すると、AWS インフラストラクチャ全体で API 呼び出しに関連するイベントをログに記録し、継続的に監視し、保持できます。詳細に関しては、 https://aws.amazon.com/jp/cloudtrail/を参照してください。 Amazon CloudWatch は、AWS クラウドリソースと AWS で実行するアプリケーションのモニタリングサービスです。Amazon CloudWatch を使用して、メトリックスを収集して追跡すること、ログファイルを収集してモニタリングすること、アラームを設定すること、および AWS リソースの変更に自動的に反応することができます。詳細に関しては、https://aws.amazon.com/jp/cloudwatch/を参照してください。 AWSはAWSシステム内でシステムとデバイス間で監査可能なイベントカテゴリを識別しています。サービスチームは監査機能を設定して、要件に従って継続的にセキュリティ関連イベントを記録しています。ログストレージシステムは、ログストレージの次のニーズが発生すると自動的に容量を増やす、スケーラブルで高可用性のサービスを提供するように設計されています。AWS内のシステムは、主要な運用メトリックスやセキュリティメトリックスをモニタリングするよう広範に実装されます。重要計測値が早期警戒しきい値を超える場合に運用管理担当者に自動的に通知されるよう、アラームが設定されています。しきい値を超えると、AWSインシデント対応プロセスが開始されます。Amazonインシデント対応チームは、業界標準の診断手順を採用して、ビジネスに影響するイベントに解決策を実行します。スタッフは24時間年中無休でインシデントの検出、影響の管理、および解決にあたっています。 AWSの役割と責任は、SOC、PCI DSS、ISO 27001、およびFedRAMPへの準拠のため、監査中に外部の独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf
6	6.1	6.1.4	(1)	(c)	情報システムセキュリティ責任者は、情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施すること。	適合可能	・情報システムセキュリティ責任者は、情報システム（業務アプリケーション）において、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施することについて、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウドの割り当て領域に対する不正侵入、不正操作等がなされていないことの検証を行うためのログについても点検又は分析の対象となるが、AWSが提供するログに関するサービス(CloudTrail、CloudWatchサービス等)の仕様上の理由等により、統一基準が求めるログの点検又は分析にかかる項目が一部制約される可能性があることに留意する。	・AWSクラウドは、AWS CloudTrail及びAWS CloudWatchサービスを提供しており、当該機能を用いることで、利用者のAWSリソースについて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無についての点検又は分析が可能である。 ・AWSはPCI DSS、ISO 27001、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無についての点検又は分析を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無についての点検又は分析を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。 ・AWSクラウドでは、アカウント侵害の可能性を示す異常な API コールや不正なデプロイなどのアクティビティを継続的にモニタリングし、悪意のある操作や不正な動作などの脅威を機械学習を用いて検出する機能を持つAmazon Guard Dutyを提供する。	AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。 CloudTrail を使用すると、AWS インフラストラクチャ全体で API 呼び出しに関連するイベントをログに記録し、継続的に監視し、保持できます。詳細に関しては、 https://aws.amazon.com/jp/cloudtrail/を参照してください。 Amazon CloudWatch は、AWS クラウドリソースと AWS で実行するアプリケーションのモニタリングサービスです。Amazon CloudWatch を使用して、メトリックスを収集して追跡すること、ログファイルを収集してモニタリングすること、アラームを設定すること、および AWS リソースの変更に自動的に反応することができます。詳細に関しては、https://aws.amazon.com/jp/cloudwatch/を参照してください。 AWSはAWSシステム内でシステムとデバイス間で監査可能なイベントカテゴリを識別しています。サービスチームは監査機能を設定して、要件に従って継続的にセキュリティ関連イベントを記録しています。ログストレージシステムは、ログストレージの次のニーズが発生すると自動的に容量を増やす、スケーラブルで高可用性のサービスを提供するように設計されています。AWS内のシステムは、主要な運用メトリックスやセキュリティメトリックスをモニタリングするよう広範に実装されます。重要計測値が早期警戒しきい値を超える場合に運用管理担当者に自動的に通知されるよう、アラームが設定されています。しきい値を超えると、AWSインシデント対応プロセスが開始されます。Amazonインシデント対応チームは、業界標準の診断手順を採用して、ビジネスに影響するイベントに解決策を実行します。スタッフは24時間年中無休でインシデントの検出、影響の管理、および解決にあたっています。 AWSの役割と責任は、SOC、PCI DSS、ISO 27001、およびFedRAMPへの準拠のため、監査中に外部の独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf Amazon GuardDuty は、AWS アカウントとワークロードを保護するために悪意のある操作や不正な動作を継続的にモニタリングする脅威検出サービスです。アカウント侵害の可能性を示す異常な API コールや不正なデプロイなどのアクティビティをモニタリングします。詳細に関しては、 https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/what-is-guardduty.htmlを参照してください。
6	6.1	6.1.5	暗号・電子署名						
6	6.1	6.1.5	(1)	暗号化機能・電子署名機能の導入					
6	6.1	6.1.5	(1)	(a)	情報システムセキュリティ責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の措置を講ずること。	適合可能	(ア)(イ)に対応する以下の記載を参照のこと。	(ア)(イ)に対応する以下の記載を参照のこと。	
6	6.1	6.1.5	(1)	(a)	(ア) 要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。	適合可能	・情報システムセキュリティ責任者は、要機密情報を取り扱う情報システム（業務アプリケーション）において、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けることについて、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・暗号化機能については、AWSクラウドの暗号化機能のほか、情報システム独自に暗号化機能を実装することも選択肢となることに留意する。	・AWSクラウドは、データの暗号化機能を提供しており、当該機能を用いることで、利用者のAWSリソースについて、要機密情報を取り扱う情報システムにおける暗号化機能の実装が可能である。 ・AWSはPCI DSS、ISO 27001、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（暗号化機能を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（暗号化機能を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	AWSにはスケーラブルで効果的な暗号化機能が提供されており、クラウド内に保管中のデータのセキュリティをより一層強化できます。これには以下が含まれます。 ☆EBS、S3、Glacier、Oracle RDS、SQL Server RDS、およびRedshiftといった、AWSのストレージおよびデータベースサービスに利用できる、データの暗号化機能 ☆暗号化キーをAWS側で管理するか、完全に自分で管理するかを選択できる、AWS Key Management Serviceなどの柔軟なキー管理オプション ☆コンプライアンスの要件を満たすことを可能にする、AWS CloudHSMを使用した専用の、ハードウェアベースの暗号化キーストレージ さらに、AWSには、AWS環境内でお客様が開発またはデプロイされたどのサービスにも暗号化とデータ保護を統合できるAPIが用意されています。詳細に関しては、 https://aws.amazon.com/jp/security/を参照してください。 AWS は、AWS インフラストラクチャ内で採用される必要な暗号化用の暗号キーを内部的に確立、管理しています。AWS は NIST で承認されたキー管理テクノロジーとプロセスを AWS 情報システムで使用して対称暗号キーを作成、管理、配布しています。対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストで必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認証をセキュリティ保護、配布するために使用されます。AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001 、および FedRAMP への AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf
6	6.1	6.1.5	(1)	(a)	(イ) 要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。	対象外	電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときに当該機能を設けることについては、クラウドサービス利用有無にかかわらず情報システムセキュリティ責任者が検討するべき事項である。	電子署名の付与及び検証を行う機能については、本リファレンスの説明の対象外。	

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
6	6.1	6.1.5	(1)	(b)	情 報システムセキュリティ責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について、以下の事項を含めて定めること。	適合可能	・情報システムセキュリティ責任者は、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様に、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システム（業務アプリケーション）で使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について、以下詳細項目(ア)(イ)(ウ)(エ)の事項を含めて定める必要がある。 [留意事項] ・AWSクラウド提供の暗号化サービスを使う場合、および、独自に暗号化機能を実装する場合のいずれも遵守する必要があることに留意する。 ・AWSクラウドでは電子署名については提供しないことを留意し、サードパーティー製品を含めて対策手段を検討することが望ましい。 ・CRYPTRECの「電子政府推奨暗号リスト」は常に更新される可能性があることを念頭に置き、AWSクラウドが提供する暗号化サービスを使う場合も、使用される暗号アルゴリズムが危殆化していないかについて、設計、構築、運用の各段階で、確認する必要があることに留意する。	・AWSクラウドは、データの暗号化機能を提供しており、当該機能を用いることで、利用者のAWSリソースについて、要機密情報を取り扱う情報システムにおける暗号化機能の実装が可能である。 ・AWSはPCI DSS、ISO 27001、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（暗号化機能を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（暗号化機能を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	AWSにはスケーラブルで効果的な暗号化機能が提供されており、クラウド内に保管中のデータのセキュリティをより一層強化できます。これには以下が含まれます。 ☆EBS、S3、Glacier、Oracle RDS、SQL Server RDS、およびRedshiftといった、AWSのストレージおよびデータベースサービスに利用できる、データの暗号化機能 ☆暗号化キーをAWS側で管理するか、完全に自分で管理するかを選択できる、AWS Key Management Serviceなどの柔軟なキー管理オプション ☆コンプライアンスの要件を満たすことを可能にする、AWS CloudHSMを使用した専用の、ハードウェアベースの暗号化キーストレージ さらに、AWSには、AWS環境内でお客様が開発またはデプロイされたどのサービスにも暗号化とデータ保護を統合できるAPIが用意されています。詳細に関しては、https://aws.amazon.com/jp/security/を参照してください。 AWS は、AWS インフラストラクチャ内で採用される必要な暗号化用の暗号キーを内部的に確立、管理しています。AWS は NIST で承認されたキー管理テクノロジーとプロセスを AWS 情報システムで使用して対称暗号キーを作成、管理、配布しています。対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストで必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認証をセキュリティ保護、配布するために使用されます。AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001 、および FedRAMP への AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf
6	6.1	6.1.5	(1)	(b)	(ア) 職員等が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させること。	適合可能	・情報システムセキュリティ責任者は、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様に、職員等が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させる必要がある。 [留意事項] ・AWSクラウド提供の暗号化サービスを使う場合、および、独自に暗号化機能を実装する場合のいずれも遵守する必要があることに留意する。 ・AWSクラウドでは電子署名については提供しないことに留意し、サードパーティー製品を含めて対策手段を検討することが望ましい。 ・CRYPTRECの「電子政府推奨暗号リスト」は常に更新される可能性があることを念頭に置き、AWSクラウドが提供する暗号化サービスを使う場合も、使用される暗号アルゴリズムが危殆化していないかについて、設計、構築、運用の各段階で、確認および対処の検討が必要となることに留意する。	・AWSクラウドは、データの暗号化機能を提供しており、当該機能を用いることで、利用者のAWSリソースについて、要機密情報を取り扱う情報システムにおける暗号化機能の実装が可能である。 ・AWSはPCI DSS、ISO 27001、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（暗号化機能を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（暗号化機能を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	AWSにはスケーラブルで効果的な暗号化機能が提供されており、クラウド内に保管中のデータのセキュリティをより一層強化できます。これには以下が含まれます。 ☆EBS、S3、Glacier、Oracle RDS、SQL Server RDS、およびRedshiftといった、AWSのストレージおよびデータベースサービスに利用できる、データの暗号化機能 ☆暗号化キーをAWS側で管理するか、完全に自分で管理するかを選択できる、AWS Key Management Serviceなどの柔軟なキー管理オプション ☆コンプライアンスの要件を満たすことを可能にする、AWS CloudHSMを使用した専用の、ハードウェアベースの暗号化キーストレージ さらに、AWSには、AWS環境内でお客様が開発またはデプロイされたどのサービスにも暗号化とデータ保護を統合できるAPIが用意されています。詳細に関しては、https://aws.amazon.com/jp/security/を参照してください。 AWS は、AWS インフラストラクチャ内で採用される必要な暗号化用の暗号キーを内部的に確立、管理しています。AWS は NIST で承認されたキー管理テクノロジーとプロセスを AWS 情報システムで使用して対称暗号キーを作成、管理、配布しています。対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストで必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認証をセキュリティ保護、配布するために使用されます。AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001 、および FedRAMP への AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf
6	6.1	6.1.5	(1)	(b)	(イ) 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「電子政府推奨暗号リスト」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用すること。	適合可能	・情報システムセキュリティ責任者は、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様に、情報システム（業務アプリケーション）の新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「電子政府推奨暗号リスト」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用する必要がある。 [留意事項] ・AWSクラウド提供の暗号化サービスを使う場合、および、独自に暗号化機能を実装する場合のいずれも遵守する必要があることに留意する。 ・AWSクラウドでは電子署名については提供しないことを留意し、サードパーティー製品を含めて対策手段を検討することが望ましい。 ・CRYPTRECの「電子政府推奨暗号リスト」は常に更新される可能性があることを念頭に置き、AWSクラウドが提供する暗号化サービスを使う場合も、使用される暗号アルゴリズムが危殆化していないかについて確認した上で採用する必要があることに留意する。	・AWSクラウドは、データの暗号化機能を提供しており、当該機能を用いることで、利用者のAWSリソースについて、要機密情報を取り扱う情報システムにおける暗号化機能の実装が可能である。 ・AWSはPCI DSS、ISO 27001、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（暗号化機能を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（暗号化機能を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	AWSにはスケーラブルで効果的な暗号化機能が提供されており、クラウド内に保管中のデータのセキュリティをより一層強化できます。これには以下が含まれます。 ☆EBS、S3、Glacier、Oracle RDS、SQL Server RDS、およびRedshiftといった、AWSのストレージおよびデータベースサービスに利用できる、データの暗号化機能 ☆暗号化キーをAWS側で管理するか、完全に自分で管理するかを選択できる、AWS Key Management Serviceなどの柔軟なキー管理オプション ☆コンプライアンスの要件を満たすことを可能にする、AWS CloudHSMを使用した専用の、ハードウェアベースの暗号化キーストレージ さらに、AWSには、AWS環境内でお客様が開発またはデプロイされたどのサービスにも暗号化とデータ保護を統合できるAPIが用意されています。詳細に関しては、https://aws.amazon.com/jp/security/を参照してください。 AWS は、AWS インフラストラクチャ内で採用される必要な暗号化用の暗号キーを内部的に確立、管理しています。AWS は NIST で承認されたキー管理テクノロジーとプロセスを AWS 情報システムで使用して対称暗号キーを作成、管理、配布しています。対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストで必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認証をセキュリティ保護、配布するために使用されます。AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001 、および FedRAMP への AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf
6	6.1	6.1.5	(1)	(b)	(ウ) 暗号化及び電子署名に使用するアルゴリズムが危殆化した場合又はそれを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定めること。	適合可能	・情報システムセキュリティ責任者は、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様に、暗号化及び電子署名に使用するアルゴリズムが危殆化した場合又はそれを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定める必要がある。 [留意事項] ・AWSクラウド提供の暗号化サービスを使う場合、および、独自に暗号化機能を実装する場合のいずれも遵守する必要があることに留意する。 ・AWSクラウドでは電子署名については提供しないことを留意し、サードパーティー製品を含めて対策手段を検討することが望ましい。	・AWSクラウドは、データの暗号化機能を提供しており、当該機能を用いることで、利用者のAWSリソースについて、要機密情報を取り扱う情報システムにおける暗号化機能の実装が可能である。 ・AWSはPCI DSS、ISO 27001、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（暗号化機能を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（暗号化機能を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	AWSにはスケーラブルで効果的な暗号化機能が提供されており、クラウド内に保管中のデータのセキュリティをより一層強化できます。これには以下が含まれます。 ☆EBS、S3、Glacier、Oracle RDS、SQL Server RDS、およびRedshiftといった、AWSのストレージおよびデータベースサービスに利用できる、データの暗号化機能 ☆暗号化キーをAWS側で管理するか、完全に自分で管理するかを選択できる、AWS Key Management Serviceなどの柔軟なキー管理オプション ☆コンプライアンスの要件を満たすことを可能にする、AWS CloudHSMを使用した専用の、ハードウェアベースの暗号化キーストレージ さらに、AWSには、AWS環境内でお客様が開発またはデプロイされたどのサービスにも暗号化とデータ保護を統合できるAPIが用意されています。詳細に関しては、https://aws.amazon.com/jp/security/を参照してください。 AWS は、AWS インフラストラクチャ内で採用される必要な暗号化用の暗号キーを内部的に確立、管理しています。AWS は NIST で承認されたキー管理テクノロジーとプロセスを AWS 情報システムで使用して対称暗号キーを作成、管理、配布しています。対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストで必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認証をセキュリティ保護、配布するために使用されます。AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001 、および FedRAMP への AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
6	6.1	6.1.5	(1)	(b)	(エ) 暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定めること。	適合可能	・情報システムセキュリティ責任者は、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様に、暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定める必要がある。 [留意事項] ・AWSクラウド提供の暗号化サービスを使う場合、および、独自に暗号化機能を実装する場合のいずれも遵守する必要があることに留意する。 ・AWSクラウドでは電子署名については提供しないことを留意し、サードパーティー製品を含めて対策手段を検討することが望ましい。	・AWSクラウドは、データの暗号化機能を提供しており、利用者は当該機能を用いることで、利用者のAWSリソースについて、要機密情報を取り扱う情報システムにおける暗号化機能の実装が可能である。 ・AWSクラウドは、マネージド型サービスAWS Key Management Service (KMS)を提供しており、利用者は当該機能を用いることで、利用者のAWSリソースについて、要機密情報を取り扱う情報システムにおける暗号化に用いる暗号化キーの管理が可能である。	AWSにはスケーラブルで効果的な暗号化機能が提供されており、クラウド内に保管中のデータのセキュリティをより一層強化できます。これには以下が含まれます。 ☆EBS、S3、Glacier、Oracle RDS、SQL Server RDS、およびRedshiftといった、AWSのストレージおよびデータベースサービスに利用できる、データの暗号化機能 ☆暗号化キーをAWS側で管理するか、完全に自分で管理するかを選択できる、AWS Key Management Serviceなどの柔軟なキー管理オプション ☆コンプライアンスの要件を満たすことを可能にする、AWS CloudHSMを使用した専用の、ハードウェアベースの暗号化キーストレージ さらに、AWSには、AWS環境内でお客様が開発またはデプロイされたどのサービスにも暗号化とデータ保護を統合できるAPIが用意されています。詳細に関しては、https://aws.amazon.com/jp/security/を参照してください。 AWS Key Management Service (KMS) とは、データの暗号化に使用する暗号化キーを簡単に作成および管理できるマネージド型サービスで、キーのセキュリティを保護するために Hardware Security Modules (HSM) を使用します。AWS Key Management Service は、AWS の他のいくつかのサービスと統合されており、これらのサービスに保存したデータが保護されます。詳細に関しては、https://aws.amazon.com/jp/kms/を参照してください。 AWS は、AWS インフラストラクチャ内で採用される必要な暗号化用の暗号キーを内部的に確立、管理しています。AWS は NIST で承認されたキー管理テクノロジーとプロセスを AWS 情報システムで使用して対称暗号キーを作成、管理、配布しています。対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストで必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認証をセキュリティ保護、配布するために使用されます。AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001 、および FedRAMP への AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf
6	6.1	6.1.5	(1)	(c)	情報システムセキュリティ責任者は、機関等における暗号化及び電子署名のアルゴリズム及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な電子証明書を政府認証基盤（GPKI）が発行している場合は、それを使用するように定めること。	対象外	機関等における暗号化及び電子署名のアルゴリズム及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な電子証明書を政府認証基盤（GPKI）が発行している場合、それを使用するように定めることについては、クラウドサービス利用有無にかかわらず情報システムセキュリティ責任者が検討するべき事項である。	適用可能な電子証明書を政府認証基盤（GPKI）が発行している場合にそれを使用するように定めることについては、本リファレンスの説明の対象外。	–
6	6.1	6.1.5	(2)	暗号化・電子署名に係る管理					
6	6.1	6.1.5	(2)	(a)	情報システムセキュリティ責任者は、暗号及び電子署名を適切な状況で利用するため、以下の措置を講ずること。	適合可能	(ア)(イ)に対応する以下の記載を参照のこと。	(ア)(イ)に対応する以下の記載を参照のこと。	
6	6.1	6.1.5	(2)	(a)	(ア) 電子署名の付与を行う情報システムにおいて、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全な方法で提供すること。	対象外	電子署名の付与を行う情報システムにおいて、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全な方法で提供することについては、クラウドサービス利用有無にかかわらず情報システムセキュリティ責任者が検討するべき事項である。	電子署名の付与及び検証を行う機能については、本リファレンスの説明の対象外。	
6	6.1	6.1.5	(2)	(a)	(イ) 暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて、暗号化又は電子署名のために選択されたアルゴリズムの危殆化及びプロトコルの脆弱性に関する情報を定期的に入手し、必要に応じて、職員等と共有を図ること。	適合可能	・情報システムセキュリティ責任者は、暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様に、暗号化又は電子署名のために選択されたアルゴリズムの危殆化及びプロトコルの脆弱性に関する情報を定期的に入手し、必要に応じて、職員等と共有を図る必要がある。 [留意事項] ・暗号化の実装手段として、AWSクラウド提供の暗号化サービスを使う場合、および、独自に機能を実装する場合のいずれも遵守する必要があることに留意する。	・AWSクラウドは、データの暗号化機能を提供しており、当該機能を用いることで、利用者のAWSリソースについて、要機密情報を取り扱う情報システムにおける暗号化機能の実装が可能である。 ・AWSはPCI DSS、ISO 27001、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（暗号化機能を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（暗号化機能を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	AWSにはスケーラブルで効果的な暗号化機能が提供されており、クラウド内に保管中のデータのセキュリティをより一層強化できます。これには以下が含まれます。 ☆EBS、S3、Glacier、Oracle RDS、SQL Server RDS、およびRedshiftといった、AWSのストレージおよびデータベースサービスに利用できる、データの暗号化機能 ☆暗号化キーをAWS側で管理するか、完全に自分で管理するかを選択できる、AWS Key Management Serviceなどの柔軟なキー管理オプション ☆コンプライアンスの要件を満たすことを可能にする、AWS CloudHSMを使用した専用の、ハードウェアベースの暗号化キーストレージ さらに、AWSには、AWS環境内でお客様が開発またはデプロイされたどのサービスにも暗号化とデータ保護を統合できるAPIが用意されています。詳細に関しては、https://aws.amazon.com/jp/security/を参照してください。 AWS は、AWS インフラストラクチャ内で採用される必要な暗号化用の暗号キーを内部的に確立、管理しています。AWS は NIST で承認されたキー管理テクノロジーとプロセスを AWS 情報システムで使用して対称暗号キーを作成、管理、配布しています。対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストで必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認証をセキュリティ保護、配布するために使用されます。AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001 、および FedRAMP への AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf
6	6.2	情報セキュリティの脅威への対策							
6	6.2	6.2.1	ソフトウェアに関する脆弱性対策						
6	6.2	6.2.1	(1)	ソフトウェアに関する脆弱性対策の実施					
6	6.2	6.2.1	(1)	(a)	情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施すること。	適合可能	・情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施するにあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウドに構築する部分（アプリケーション等）については、情報システムセキュリティ責任者が脆弱性対策を実施する必要があることに留意する。 ・AWSクラウドにおいて、RDS(リレーショナルデータベースサービス）等に対するセキュリティパッチ適用はAWSクラウド側にて自動的に行われる。ただし、EC2上のOSやアプリケーションのセキュリティを担保する責任は情報システムセキュリティ責任者側にあることに留意する。	・AWSはPCI DSS、ISO 27001、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（利用ソフトウェアに関する脆弱性対策を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（利用ソフトウェアに関する脆弱性対策を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。 ・AWSクラウドでは、Amazon Inspector、AWS WAFを提供する。 -Amazon Inspector…自動化されたセキュリティ評価によって、アプリケーションのセキュリティ脆弱性やベストプラクティスからの逸脱を特定する機能を提供する。 -AWS WAF…アプリケーションの可用性に対する影響、セキュリティの侵害、過剰なリソース消費を生じる可能性がある一般的なウェブエクスプロイトからウェブアプリケーションを保護するために役立つウェブアプリケーションファイアウォール機能を提供する。	AWSネットワーク管理は、SOC、PCI DSS、ISO 27001、およびFedRAMPへのAWSの継続的な準拠の一環として、第三者の独立監査人によって定期的に確認されます。 AWSは、そのインフラストラクチャコンポーネントを通じて最小権限を実装しています。また、特定のビジネス目的を持っていないすべてのポートとプロトコルを禁止しています。AWS は、デバイスの使用に不可欠な機能のみの最小実装という厳格な手法に従っています。ネットワークスキャンを実行し、不要なポートまたはプロトコルが使用されている場合は修正されます。 AWS環境内のホストオペレーティングシステム、ウェブアプリケーション、およびデータベースでさまざまなツールを利用した、定期的な内外部の脆弱性のスキャンが実行されます。脆弱性のスキャンと解決手法は、AWSのPCI DSSおよびFedRAMPへの継続的な準拠の一環として定期的に確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf Amazon InspectorはAWS にデプロイされたアプリケーションのセキュリティとコンプライアンスを向上させるための、自動化されたセキュリティ評価サービスです。自動的にアプリケーションを評価し、脆弱性やベストプラクティスからの逸脱がないかどうかを確認します。評価が実行された後、重大性の順にセキュリティの調査結果を示した詳細なリストが Amazon Inspector によって作成されます。 詳細に関しては、 https://aws.amazon.com/jp/inspector/ を参照してください。 AWS WAF は、アプリケーションの可用性に対する影響、セキュリティの侵害、過剰なリソース消費を生じる可能性がある一般的なウェブエクスプロイトからウェブアプリケーションを保護するために役立つウェブアプリケーションファイアウォールです。AWS WAF では、カスタマイズ可能なウェブセキュリティルールを定義することによって、ウェブアプリケーションに対するどのトラフィックを許可またはブロックするかを制御できます。AWS WAF は、SQL インジェクションまたはクロスサイトスクリプティングなどの一般的な攻撃パターンをブロックするカスタムルール、および特定のアプリケーションのために設計されたルールを作成するために使用できます。詳細に関してはhttps://aws.amazon.com/jp/waf/を参照してください。

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
6	6.2	6.2.1	(1)	(b)	情報システムセキュリティ責任者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上でとり得る対策がある場合は、当該対策を実施すること。	適合可能	・情報システムセキュリティ責任者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上でとり得る対策がある場合に、当該対策を実施するにあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウドに構築する部分（アプリケーション等）については、情報システムセキュリティ責任者が脆弱性対策を実施する必要があることに留意する。 ・AWSクラウドにおいて、OSやRDS(リレーショナルデータベースサービス）等に対するセキュリティパッチ適用はAWSクラウド側にて自動的に行われる。ただし、EC2上のOSやアプリケーションのセキュリティを担保する責任は情報システムセキュリティ責任者側にあることに留意する。	・AWSはPCI DSS、ISO 27001、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（利用ソフトウェアに関する脆弱性対策を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（利用ソフトウェアに関する脆弱性対策を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。 ・AWSクラウドでは、Amazon Guard Duty、AWS WAFを提供する。 -Amazon Guard Duty…アカウント侵害の可能性を示す異常な API コールや不正なデプロイなどのアクティビティを継続的にモニタリングし、悪意のある操作や不正な動作などの脅威を機械学習を用いて検出する機能を提供する。 -AWS WAF…アプリケーションの可用性に対する影響、セキュリティの侵害、過剰なリソース消費を生じる可能性がある一般的なウェブエクスプロイトからウェブアプリケーションを保護するために役立つウェブアプリケーションファイアウォール機能を提供する。	AWSネットワーク管理は、SOC、PCI DSS、ISO 27001、およびFedRAMPへのAWSの継続的な準拠の一環として、第三者の独立監査人によって定期的に確認されます。 AWSは、そのインフラストラクチャコンポーネントを通じて最小権限を実装しています。また、特定のビジネス目的を持っていないすべてのポートとプロトコルを禁止しています。AWS は、デバイスの使用に不可欠な機能のみの最小実装という厳格な手法に従っています。ネットワークスキャンを実行し、不要なポートまたはプロトコルが使用されている場合は修正されます。 AWS環境内のホストオペレーティングシステム、ウェブアプリケーション、およびデータベースでさまざまなツールを利用した、定期的な内外部の脆弱性のスキャンが実行されます。脆弱性のスキャンと解決手法は、AWSのPCI DSSおよびFedRAMPへの継続的な準拠の一環として定期的に確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf Amazon GuardDuty は、AWS アカウントとワークロードを保護するために悪意のある操作や不正な動作を継続的にモニタリングする脅威検出サービスです。アカウント侵害の可能性を示す異常な API コールや不正なデプロイなどのアクティビティをモニタリングします。詳細に関しては、 https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/what-is-guardduty.htmlを参照してください。 AWS WAF は、アプリケーションの可用性に対する影響、セキュリティの侵害、過剰なリソース消費を生じる可能性がある一般的なウェブエクスプロイトからウェブアプリケーションを保護するために役立つウェブアプリケーションファイアウォールです。AWS WAF では、カスタマイズ可能なウェブセキュリティルールを定義することによって、ウェブアプリケーションに対するどのトラフィックを許可またはブロックするかを制御できます。AWS WAF は、SQL インジェクションまたはクロスサイトスクリプティングなどの一般的な攻撃パターンをブロックするカスタムルール、および特定のアプリケーションのために設計されたルールを作成するために使用できます。詳細に関してはhttps://aws.amazon.com/jp/waf/を参照してください。
6	6.2	6.2.1	(1)	(c)	情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアにおける脆弱性対策の状況を定期的に確認すること。	適合可能	・情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアにおける脆弱性対策の状況を定期的に確認するにあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い、従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウドに構築する部分（アプリケーション等）については情報システムセキュリティ責任者が脆弱性対策の状況を定期的に確認する必要があることに留意する。 ・AWSクラウドにおいて、OSやRDS(リレーショナルデータベースサービス）等に対するセキュリティパッチ適用はAWSクラウド側にて自動的に行われる。ただし、EC2上のOSやアプリケーションのセキュリティを担保する責任は情報システムセキュリティ責任者側にあることに留意する。	・AWSはPCI DSS、ISO 27001、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（利用ソフトウェアに関する脆弱性対策を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（利用ソフトウェアに関する脆弱性対策を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。 ・AWSクラウドでは、Amazon Inspector、AWS Trusted Advisorを提供する。 -Amazon Inspector…自動化されたセキュリティ評価によって、アプリケーションのセキュリティ脆弱性やベストプラクティスからの逸脱を特定する機能を提供する。 -AWS Trusted Advisor…現在のAWSインフラストラクチャのプロビジョニング状態と ベストプラクティスを比較し、リアルタイムに評価を行う機能を提供する。	Amazon InspectorはAWS にデプロイされたアプリケーションのセキュリティとコンプライアンスを向上させるための、自動化されたセキュリティ評価サービスです。自動的にアプリケーションを評価し、脆弱性やベストプラクティスからの逸脱がないかどうかを確認します。評価が実行された後、重大性の順にセキュリティの調査結果を示した詳細なリストが Amazon Inspector によって作成されます。 詳細に関しては、 https://aws.amazon.com/jp/inspector/ を参照してください。 AWS Trusted AdvisorはAWS 環境を最適化することで、コスト削減、パフォーマンスの向上、セキュリティの向上に役立つオンラインリソースです。Trusted Advisorでは、AWSベストプラクティスに従ってリソースをプロビジョニングするのに役立つ、リアルタイムガイダンスを提供しています。 詳細に関しては、https://aws.amazon.com/jp/premiumsupport/trustedadvisor/ を参照してください。
6	6.2	6.2.1	(1)	(d)	情報システムセキュリティ責任者は、脆弱性対策の状況の定期的な確認により、脆弱性対策が講じられていない状態が確認された場合並びにサーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずること。	適合可能	・情報システムセキュリティ責任者は、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様に、脆弱性対策の状況の定期的な確認により、脆弱性対策が講じられていない状態が確認された場合並びにサーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずる必要がある。 [留意事項] ・AWSクラウドに構築する部分（アプリケーション等）については、情報システムセキュリティ責任者がセキュリティパッチ適用等の措置を実施する必要があることに留意する。 ・AWSクラウドにおいて、OSやRDS(リレーショナルデータベースサービス）等に対するセキュリティパッチ適用はAWSクラウド側にて自動的に行われる。ただし、EC2上のOSやアプリケーションのセキュリティを担保する責任は情報システムセキュリティ責任者側にあることに留意する。	・AWSはPCI DSS、ISO 27001、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（セキュリティパッチ適用を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（セキュリティパッチ適用を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	AWSは、ハイパーバイザおよびネットワーキングサービスなど、お客様へのサービス提供をサポートするシステムにパッチを適用する責任を持ちます。この処理は、AWSポリシーに従い、またISO 27001、NIST、およびPCIの要件に準拠して、必要に応じて実行します。お客様が使用しているゲストオペレーティングシステム、ソフトウェア、およびアプリケーションの統制については、お客様が行い、お客様がそれらのシステムにパッチを適用する責任を持ちます。 詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf
6	6.2	6.2.2	不正プログラム対策						
6	6.2	6.2.2	(1)	不正プログラム対策の実施					
6	6.2	6.2.2	(1)	(a)	情報システムセキュリティ責任者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入すること。ただし、当該サーバ装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除く。	適合可能	・情報システムセキュリティ責任者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入することについて、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウドに構築する部分については、情報システムセキュリティ責任者が不正プログラム対策を実施する必要があることに留意する。	・AWSはPCI DSS、ISO 27001、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（不正プログラムへの対策を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（不正プログラムへの対策を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	AWSネットワーク管理は、SOC、PCI DSS、ISO 27001、およびFedRAMPへのAWSの継続的な準拠の一環として、第三者の独立監査人によって定期的に確認されます。 AWSは、そのインフラストラクチャコンポーネントを通じて最小権限を実装しています。また、特定のビジネス目的を持っていないすべてのポートとプロトコルを禁止しています。AWS は、デバイスの使用に不可欠な機能のみの最小実装という厳格な手法に従っています。ネットワークスキャンを実行し、不要なポートまたはプロトコルが使用されている場合は修正されます。 AWS環境内のホストオペレーティングシステム、ウェブアプリケーション、およびデータベースでさまざまなツールを利用した、定期的な内外部の脆弱性のスキャンが実行されます。脆弱性のスキャンと解決手法は、AWSのPCI DSSおよびFedRAMPへの継続的な準拠の一環として定期的に確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
6	6.2	6.2.2	(1)	(b)	情報システムセキュリティ責任者は、想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講ずること。	適合可能	・情報システムセキュリティ責任者は、想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講ずることについて、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウドに構築する部分については、情報システムセキュリティ責任者が不正プログラム対策を実施する必要があることに留意する。	・AWSはPCI DSS、ISO 27001、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（不正プログラムへの対策を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（不正プログラムへの対策を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	AWSネットワーク管理は、SOC、PCI DSS、ISO 27001、およびFedRAMPへのAWSの継続的な準拠の一環として、第三者の独立監査人によって定期的に確認されます。 AWSは、そのインフラストラクチャコンポーネントを通じて最小権限を実装しています。また、特定のビジネス目的を持っていないすべてのポートとプロトコルを禁止しています。AWS は、デバイスの使用に不可欠な機能のみの最小実装という厳格な手法に従っています。ネットワークスキャンを実行し、不要なポートまたはプロトコルが使用されている場合は修正されます。 AWS環境内のホストオペレーティングシステム、ウェブアプリケーション、およびデータベースでさまざまなツールを利用した、定期的な内外部の脆弱性のスキャンが実行されます。脆弱性のスキャンと解決手法は、AWSのPCI DSSおよびFedRAMPへの継続的な準拠の一環として定期的に確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf
6	6.2	6.2.2	(1)	(c)	情報システムセキュリティ責任者は、不正プログラム対策の状況を適宜把握し、必要な対処を行うこと。	適合可能	・情報システムセキュリティ責任者は、不正プログラム対策の状況を適宜把握し、必要な対処を行うことについて、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウドに構築する部分については、情報システムセキュリティ責任者が不正プログラム対策を実施する必要があることに留意する。	・AWSはPCI DSS、ISO 27001、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（不正プログラムへの対策を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（不正プログラムへの対策を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	AWSネットワーク管理は、SOC、PCI DSS、ISO 27001、およびFedRAMPへのAWSの継続的な準拠の一環として、第三者の独立監査人によって定期的に確認されます。 AWSは、そのインフラストラクチャコンポーネントを通じて最小権限を実装しています。また、特定のビジネス目的を持っていないすべてのポートとプロトコルを禁止しています。AWS は、デバイスの使用に不可欠な機能のみの最小実装という厳格な手法に従っています。ネットワークスキャンを実行し、不要なポートまたはプロトコルが使用されている場合は修正されます。 AWS環境内のホストオペレーティングシステム、ウェブアプリケーション、およびデータベースでさまざまなツールを利用した、定期的な内外部の脆弱性のスキャンが実行されます。脆弱性のスキャンと解決手法は、AWSのPCI DSSおよびFedRAMPへの継続的な準拠の一環として定期的に確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf
6	6.2	6.2.3	サービス不能攻撃対策						
6	6.2	6.2.3	(1)	サービス不能攻撃対策の実施					
6	6.2	6.2.3	(1)	(a)	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける情報システムに限る。以下本条において同じ。）については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行うこと。	適合可能	・情報システムセキュリティ責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける情報システムに限る。以下本条において同じ。）のサービス不能攻撃対策について、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・当該システムに要求される可用性を考慮した上で、AWS標準提供のDoS対策、およびDDoS対策（AWSオプション提供のDDoS軽減対策や、その他のベンダ提供の対策等）について、導入を検討する必要があることに留意する。	AWSクラウドは、以下に示す機能やサービスを提供しており、当該機能を用いることで、利用者のAWSリソースについて、サービス不能攻撃への対策が可能である。 ・AWSはセキュリティモニタリングツールにより数種類のDoS攻撃の特定ができ、DoS攻撃が確認されるとAWSのインシデントレスポンスが開始される仕組みがあるなど、DoS攻撃による被害を低減する機能を提供している。 ・AWSは、Auto scaling, CloudFront, Route 53などのDDoS攻撃による被害を軽減するサービスを提供している。 ・マネージド型の分散サービス妨害 (DDoS) に対する保護サービスであるAWS Shieldは、AWS で実行されるアプリケーションを自動で保護する機能を提供している。AWS Shield Standardは追加費用なしでデフォルトで適用されており、ウェブサイトやアプリケーションを標的にした、最も一般的で頻繁に発生するネットワークおよびトランスポートレイヤーの DDoS 攻撃を防御することが可能である。	AWSのセキュリティモニタリングツールは、分散型のフラッディング攻撃、およびソフトウェア/ロジックによる攻撃を含む、数種類のサービス妨害（DoS）攻撃の特定に役立ちます。DoS攻撃が確認されると、AWSのインシデントレスポンスプロセスが開始されます。DoS予防ツールに加えて、各リージョンの豊富な通信プロバイダや容量の増設によりDoS攻撃を予防します。 Amazon APIエンドポイントは、Amazonを世界最大のインターネットショッピング業者にしたエンジニアリングの専門知識を参考にして、大規模で、インターネット規模の、ワールドクラスのインフラストラクチャにホストされています。専属的なDDoS緩和技術が使用されています。さらに、AWSネットワークは、複数のプロバイダによるマルチホーム構成になっていて、インターネットアクセスの多様化を実現しています。　　詳細に関しては「セキュリティプロセスの概要（2014年11月）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf AWSのお客様はAWSサービスの利点や組み込みのテクノロジーを基礎から活用して、DDoS攻撃に対する耐障害性を実現しています。 AWSサービスの組み合わせを使用して深層防御戦略を実装し、DDoS攻撃を阻止することができます。DDoSへの自動応答を行うように設計されたサービスは、影響の軽減や削減までの時間を最小化するうえで役立ちます。分散サービス妨害攻撃の軽減のための、Auto scaling、Amazon CloudFront、Amazon Route 53といったAWSテクノロジーが利用可能です。詳細に関しては、https://aws.amazon.com/jp/security/を参照してください。 AWS Shield はマネージド型の分散サービス妨害 (DDoS) に対する保護サービスで、AWS で実行しているアプリケーションを保護します。AWS Shield ではアプリケーションのダウンタイムとレイテンシーを最小限に抑える常時稼働の検出と自動インライン緩和策を提供しているため、DDoS 保護のメリットを受けるために AWS サポートに依頼する必要はありません。詳細に関しては、https://aws.amazon.com/jp/shield/　を参照してください。
6	6.2	6.2.3	(1)	(b)	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合の影響を最小とする手段を備えた情報システムを構築すること。	適合可能	・情報システムセキュリティ責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける情報システムに限る。以下本条において同じ。）がサービス不能攻撃を受けた場合の影響を最小とする手段について、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・実際にサービス不能攻撃を受けた場合を想定し、一時的な通信の制限や、段階的な緩和の対処ができるように、AWS標準提供のDoS対策、およびDDoS対策（AWSオプション提供のDDoS軽減対策や、その他のベンダ提供の対策等）について、設計・構築・運用を検討する必要があることに留意する。	AWSクラウドは、以下に示す機能やサービスを提供しており、当該機能を用いることで、利用者のAWSリソースについて、サービス不能攻撃への対策が可能である。 ・AWSはセキュリティモニタリングツールにより数種類のDoS攻撃の特定ができ、DoS攻撃が確認されるとAWSのインシデントレスポンスが開始される仕組みがあるなど、DoS攻撃による被害を低減する機能を提供している。 ・AWSは、Auto scaling, CloudFront, Route 53などのDDoS攻撃による被害を軽減するサービスを提供している。 ・マネージド型の分散サービス妨害 (DDoS) に対する保護サービスであるAWS Shieldは、AWS で実行されるアプリケーションを自動で保護する機能を提供している。AWS Shield Standardは追加費用なしでデフォルトで適用されており、ウェブサイトやアプリケーションを標的にした、最も一般的で頻繁に発生するネットワークおよびトランスポートレイヤーの DDoS 攻撃を防御することが可能である。	AWSのセキュリティモニタリングツールは、分散型のフラッディング攻撃、およびソフトウェア/ロジックによる攻撃を含む、数種類のサービス妨害（DoS）攻撃の特定に役立ちます。DoS攻撃が確認されると、AWSのインシデントレスポンスプロセスが開始されます。DoS予防ツールに加えて、各リージョンの豊富な通信プロバイダや容量の増設によりDoS攻撃を予防します。 Amazon APIエンドポイントは、Amazonを世界最大のインターネットショッピング業者にしたエンジニアリングの専門知識を参考にして、大規模で、インターネット規模の、ワールドクラスのインフラストラクチャにホストされています。専属的なDDoS緩和技術が使用されています。さらに、AWSネットワークは、複数のプロバイダによるマルチホーム構成になっていて、インターネットアクセスの多様化を実現しています。　　詳細に関しては「セキュリティプロセスの概要（2014年11月）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf AWSのお客様はAWSサービスの利点や組み込みのテクノロジーを基礎から活用して、DDoS攻撃に対する耐障害性を実現しています。 AWSサービスの組み合わせを使用して深層防御戦略を実装し、DDoS攻撃を阻止することができます。DDoSへの自動応答を行うように設計されたサービスは、影響の軽減や削減までの時間を最小化するうえで役立ちます。分散サービス妨害攻撃の軽減のための、Auto scaling、Amazon CloudFront、Amazon Route 53といったAWSテクノロジーが利用可能です。詳細に関しては、https://aws.amazon.com/jp/security/を参照してください。 AWS Shield はマネージド型の分散サービス妨害 (DDoS) に対する保護サービスで、AWS で実行しているアプリケーションを保護します。AWS Shield ではアプリケーションのダウンタイムとレイテンシーを最小限に抑える常時稼働の検出と自動インライン緩和策を提供しているため、DDoS 保護のメリットを受けるために AWS サポートに依頼する必要はありません。詳細に関しては、https://aws.amazon.com/jp/shield/　を参照してください。

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
6	6.2	6.2.3	(1)	(c)	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視すること。	適合可能	・情報システムセキュリティ責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける情報システムに限る。以下本条において同じ。）がサービス不能攻撃を受けることを想定した監視対象の特定について、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・実際にサービス不能攻撃を受けた場合を想定し、AWS標準提供のDoS対策、およびDDoS対策（AWSオプション提供のDDoS軽減対策や、その他のベンダ提供の対策等）について、監視対象箇所を検討する必要があることに留意する。	AWSクラウドは、以下に示す機能やサービスを提供しており、当該機能を用いることで、利用者のAWSリソースについて、サービス不能攻撃への対策が可能である。 ・AWSはセキュリティモニタリングツールにより数種類のDoS攻撃の特定ができ、DoS攻撃が確認されるとAWSのインシデントレスポンスが開始される仕組みがあるなど、DoS攻撃による被害を低減する機能を提供している。 ・AWSは、Auto scaling, CloudFront, Route 53などのDDoS攻撃による被害を軽減するサービスを提供している。	AWSのセキュリティモニタリングツールは、分散型のフラッディング攻撃、およびソフトウェア/ロジックによる攻撃を含む、数種類のサービス妨害（DoS）攻撃の特定に役立ちます。DoS攻撃が確認されると、AWSのインシデントレスポンスプロセスが開始されます。DoS予防ツールに加えて、各リージョンの豊富な通信プロバイダや容量の増設によりDoS攻撃を予防します。 Amazon APIエンドポイントは、Amazonを世界最大のインターネットショッピング業者にしたエンジニアリングの専門知識を参考にして、大規模で、インターネット規模の、ワールドクラスのインフラストラクチャにホストされています。専属的なDDoS緩和技術が使用されています。さらに、AWSネットワークは、複数のプロバイダによるマルチホーム構成になっていて、インターネットアクセスの多様化を実現しています。　　詳細に関しては「セキュリティプロセスの概要（2014年11月）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf AWSのお客様はAWSサービスの利点や組み込みのテクノロジーを基礎から活用して、DDoS攻撃に対する耐障害性を実現しています。 AWSサービスの組み合わせを使用して深層防御戦略を実装し、DDoS攻撃を阻止することができます。DDoSへの自動応答を行うように設計されたサービスは、影響の軽減や削減までの時間を最小化するうえで役立ちます。分散サービス妨害攻撃の軽減のための、Auto scaling、Amazon CloudFront、Amazon Route 53といったAWSテクノロジーが利用可能です。詳細に関しては、https://aws.amazon.com/jp/security/を参照してください。
6	6.2	6.2.4	標的型攻撃対策						
6	6.2	6.2.4	(1)	標的型攻撃対策の実施					
6	6.2	6.2.4	(1)	(a)	情報システムセキュリティ責任者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講ずること。	適合可能	・情報システムセキュリティ責任者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講ずることについて、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・標的型攻撃対策の具体的な手段（対策ソフトウェア等）によっては、クラウド構成を想定していないものもあり得るため、機能に制約が生じる可能性があることを考慮して、対策手段を検討する必要があることに留意する。。 ・AWS クラウドを利用する場合、AWS WAF も対策の選択肢となるが、システム特性を踏まえたユーザによる追加の設定が必要であることに留意し、サードパーティー製品を含めて対策手段を検討することが望ましい。 ・クラウド基盤部分への対策についてはユーザが実施できないため、クラウド分野のセキュリティ認証の取得状況等から勘案した上で、情報システムセキュリティ責任者がクラウドサービスを選択する必要があることに留意する。	・AWSはPCI DSS、ISO 27001、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（AWSのネットワークファイアウォール、Amazonの端末における不正プログラム対策を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（AWSのネットワークファイアウォール、Amazonの端末における不正プログラム対策を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。 ・AWSクラウドでは、アプリケーションの可用性に対する影響、セキュリティの侵害、過剰なリソース消費を生じる可能性がある一般的なウェブエクスプロイトからウェブアプリケーションを保護するために役立つウェブアプリケーションファイアウォール機能を持つAWS WAFを提供する。	ウイルス対策および悪意のあるソフトウェア対策に関する AWS のプログラム、プロセス、および手続きは、ISO 27001 基準に合わせています。詳細については、AWS SOC 1 Type II レポートを参照してください。 Amazon の資産（ノートパソコンなど）は、E メールのフィルタリングとマルウェア検出を含むウイルス対策ソフトウェアで設定されています。 AWS ネットワークファイアウォール管理および Amazon のウイルス対策プログラムは、SOC、PCI DSS、ISO 27001、および FedRAMP への AWS の継続的な準拠の一環として、第三者の独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf AWS WAF は、アプリケーションの可用性に対する影響、セキュリティの侵害、過剰なリソース消費を生じる可能性がある一般的なウェブエクスプロイトからウェブアプリケーションを保護するために役立つウェブアプリケーションファイアウォールです。AWS WAF では、カスタマイズ可能なウェブセキュリティルールを定義することによって、ウェブアプリケーションに対するどのトラフィックを許可またはブロックするかを制御できます。AWS WAF は、SQL インジェクションまたはクロスサイトスクリプティングなどの一般的な攻撃パターンをブロックするカスタムルール、および特定のアプリケーションのために設計されたルールを作成するために使用できます。詳細に関してはhttps://aws.amazon.com/jp/waf/を参照してください。
6	6.2	6.2.4	(1)	(b)	情報システムセキュリティ責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）を講ずること。	適合可能	・情報システムセキュリティ責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）を講ずることについて、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・標的型攻撃対策の具体的な手段（対策ソフトウェア等）によっては、クラウド構成を想定していないものもあり得るため、機能に制約が生じる可能性があることを考慮して、対策手段を検討する必要があることに留意する。 ・クラウド基盤部分への対策についてはユーザが実施できないため、クラウド分野のセキュリティ認証の取得状況等から勘案した上で、情報システムセキュリティ責任者がクラウドサービスを選択する必要があることに留意する。	・AWSはPCI DSS、ISO 27001、およびFedRAMPに準拠して、AWSグローバルインフラストラクチャの運用（AWSのネットワークファイアウォール、Amazonの端末における不正プログラム対策を含む）を行っており、利用者はこれらの認証を取得していることを確認可能である。 ・AWSグローバルインフラストラクチャの運用（AWSのネットワークファイアウォール、Amazonの端末における不正プログラム対策を含む）について、利用者はSOCレポートにて独立監査人によって保証されていることを確認可能である。	ウイルス対策および悪意のあるソフトウェア対策に関する AWS のプログラム、プロセス、および手続きは、ISO 27001 基準に合わせています。詳細については、AWS SOC 1 Type II レポートを参照してください。 Amazon の資産（ノートパソコンなど）は、E メールのフィルタリングとマルウェア検出を含むウイルス対策ソフトウェアで設定されています。 AWS ネットワークファイアウォール管理および Amazon のウイルス対策プログラムは、SOC、PCI DSS、ISO 27001、および FedRAMP への AWS の継続的な準拠の一環として、第三者の独立監査人によって確認されます。詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf
6	6.3	アプリケーション・コンテンツの作成・提供							
6	6.3	6.3.1	アプリケーション・コンテンツの作成時の対策						
6	6.3	6.3.1	(1)	アプリケーション・コンテンツの作成に係る規定の整備					
6	6.3	6.3.1	(1)	(a)	統括情報セキュリティ責任者は、アプリケーション・コンテンツの提供時に機関等外の情報セキュリティ水準の低下を招く行為を防止するための規定を整備すること。	対象外			
6	6.3	6.3.1	(2)	アプリケーション・コンテンツのセキュリティ要件の策定					
6	6.3	6.3.1	(2)	(a)	情報システムセキュリティ責任者は、機関等外の情報システム利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション・コンテンツについて以下の内容を仕様に含めること。	対象外			
6	6.3	6.3.1	(2)	(a)	(ア) 提供するアプリケーション・コンテンツが不正プログラムを含まないこと。	対象外			
6	6.3	6.3.1	(2)	(a)	(イ) 提供するアプリケーションが脆弱性を含まないこと。	対象外			
6	6.3	6.3.1	(2)	(a)	(ウ) 実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き、実行プログラムの形式でコンテンツを提供しないこと。	対象外			
6	6.3	6.3.1	(2)	(a)	(エ) 電子証明書を用いた署名等、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段をアプリケーション・コンテンツの提供先に与えること。	対象外			
6	6.3	6.3.1	(2)	(a)	(オ) 提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、OS やソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。	対象外			
6	6.3	6.3.1	(2)	(a)	(カ) サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。	対象外			
6	6.3	6.3.1	(2)	(b)	職員等は、アプリケーション・コンテンツの開発・作成を外部委託する場合において、前項各号に掲げる内容を調達仕様に含めること。	対象外			

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
6	6.3	6.3.2	アプリケーション・コンテンツ提供時の対策						
6	6.3	6.3.2	(1)	政府ドメイン名の使用					
6	6.3	6.3.2	(1)	(a)	情報システムセキュリティ責任者は、機関等外向けに提供するウェブサイト等が実際の機関等提供のものであることを利用者が確認できるように、政府ドメイン名を情報システムにおいて使用すること。ただし、次に掲げる場合を除く。	対象外			
6	6.3	6.3.2	(1)	(a)	(ア) 指定法人が政府ドメイン名を登録する資格を持たない場合。この場合において、当該法人は、組織の属性が資格条件となっており、不特定の個人及び組織が取得することのできないドメイン名を使用すること。	対象外			
6	6.3	6.3.2	(1)	(a)	(イ) 独立行政法人及び指定法人のうち教育機関である法人が、高等教育機関向けのドメイン名を使用する場合。この場合において、当該法人は、あらかじめ、情報セキュリティの確保の観点から、政府ドメイン名と高等教育機関向けのドメイン名のどちらを使用するべきかを比較考慮の上、判断すること。	対象外			
6	6.3	6.3.2	(1)	(a)	(ウ) 4.1.3 に掲げるソーシャルメディアサービスによる情報発信を行う場合	対象外			
6	6.3	6.3.2	(1)	(b)	職員等は、機関等外向けに提供するウェブサイト等の作成を外部委託する場合においては、前項各号列記以外の部分、同項(ア)及び(イ)の規定に則り当該機関等に適するドメイン名を使用するよう調達仕様に含めること。	対象外			
6	6.3	6.3.2	(2)	不正なウェブサイトへの誘導防止					
6	6.3	6.3.2	(2)	(a)	情報システムセキュリティ責任者は、利用者が検索サイト等を経由して機関等のウェブサイトになりすました不正なウェブサイトへ誘導されないよう対策を講ずること。	対象外			
6	6.3	6.3.2	(3)	アプリケーション・コンテンツの告知					
6	6.3	6.3.2	(3)	(a)	職員等は、アプリケーション・コンテンツを告知する場合は、告知する対象となるアプリケーション・コンテンツに利用者が確実に誘導されるよう、必要な措置を講ずること。	対象外			
6	6.3	6.3.2	(3)	(b)	職員等は、機関等外の者が提供するアプリケーション・コンテンツを告知する場合は、告知するURL 等の有効性を保つこと。	対象外			
7	情報システムの構成要素								
7	7.1	端末・サーバ装置等							
7	7.1	7.1.1	端末						
7	7.1	7.1.1	(1)	端末の導入時の対策					
7	7.1	7.1.1	(1)	(a)	情報システムセキュリティ責任者は、要保護情報を取り扱う端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。	対象外			
					（削除）	対象外			
7	7.1	7.1.1	(1)	(b)	情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。	対象外			
7	7.1	7.1.1	(2)	端末の運用時の対策					
7	7.1	7.1.1	(2)	(a)	情報システムセキュリティ責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。	対象外			
7	7.1	7.1.1	(2)	(b)	情報システムセキュリティ責任者は、所管する範囲の端末で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図ること。	対象外			
7	7.1	7.1.1	(3)	端末の運用終了時の対策					
7	7.1	7.1.1	(3)	(a)	情報システムセキュリティ責任者は、端末の運用を終了する際に、端末の電磁的記録媒体の全ての情報を抹消すること。	対象外			
7	7.1	7.1.1	(4)	要機密情報を取り扱う機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給		対象外			
7	7.1	7.1.1	(4)	(a)	統括情報セキュリティ責任者は、要機密情報を取り扱う機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末について、以下の安全管理措置に関する規定を整備すること。	対象外			
7	7.1	7.1.1	(4)	(a)	(ア) 盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置	対象外			
7	7.1	7.1.1	(4)	(a)	(イ) 機関等支給以外の端末において不正プログラムの感染等により情報窃取されることを防止するための利用時の措置	対象外			
7	7.1	7.1.1	(4)	(b)	情報セキュリティ責任者は、機関等支給以外の端末を用いた機関等の業務に係る情報処理に関する安全管理措置の実施状況を管理する責任者（以下「端末管理責任者」という。）を定めること。	対象外			
7	7.1	7.1.1	(4)	(c)	次の各号に掲げる責任者は、職員等が当該各号に定める端末を用いて要機密情報を取り扱う場合は、当該端末について(a)(ア)の安全管理措置を講ずること。	対象外			
7	7.1	7.1.1	(4)	(c)	(ア) 情報システムセキュリティ責任者 機関等が支給する端末（要管理対策区域外で使用する場合に限る）	対象外			
7	7.1	7.1.1	(4)	(c)	(イ) 端末管理責任者 機関等支給以外の端末	対象外			
7	7.1	7.1.1	(4)	(d)	端末管理責任者は、要機密情報を取り扱う機関等支給以外の端末について、前項の規定にかかわらず(a)(ア)に定める安全管理措置のうち自ら講ずることができないもの、及び(a)(イ)に定める安全管理措置を職員等に講じさせること。	対象外			
7	7.1	7.1.1	(4)	(e)	職員等は、要機密情報を取り扱う機関等支給以外の端末について、前項において(a)(ア)に定める安全管理措置のうち端末管理責任者が講ずることができないもの、及び(a)(イ)に定める安全管理措置を講ずること。	対象外			
7	7.1	7.1.2	サーバ装置						
7	7.1	7.1.2	(1)	サーバ装置の導入時の対策					

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
7	7.1	7.1.2	(1)	(a)	情報システムセキュリティ責任者は、要保護情報を取り扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。	適合可能	・AWSが取得しているISO27001等の認証で要保護情報を取り扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を確認の上、ユーザでAWSクラウドを利用した物理的な脅威から保護するための対策を選択する。	・AWSは、ISO27001等に準拠して、要保護情報を取り扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威からの保護を行っており、利用者は、これらの認証を取得していることを確認可能である。なお、AWSは、第三者による審査・監査等により、この基準への準拠について認証を取得済みである。 ・AWS のデータセンターでは、物理的および環境のセキュリティとして以下のような対策を実施している。これらの対策により、サーバ装置の盗難、不正な持ち出し、サーバ装置の不正な操作等を防止することが可能。 -ビデオ監視カメラ、侵入検出システム -データセンターのフロアへのアクセス時の2 要素認証 -身分証明書の提示、署名、権限者の付き添い -データセンターへのすべての物理的アクセスを記録、監査 -特権を必要とする作業完了後アクセス権を速やかに取消し -AWS専有インベントリ管理ツールにて、資産の追跡および監視を行い、在庫の監査を定期的に実施。	データセンター セキュリティ 資産管理 ISO 27001基準に合わせて、AWSの担当者がAWS専有インベントリ管理ツールを使用して、AWSハードウェアの資産に所有者を割り当て、追跡および監視を行っています。AWSの調達およびサプライチェーンチームは、すべてのAWSサプライヤとの関係を維持しています。 詳細については、ISO 27001基準の付録A、ドメイン7.1を参照してください。AWSは、ISO 27001認定基準への対応を確認する独立監査人から、検証および認定を受けています。 詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf 物理的および環境のセキュリティ Amazon のデータセンターは最新式で、革新的で建築的かつ工学的アプローチを採用しています。Amazon は大規模データセンターの設計、構築、運用において、長年の経験を有しています。この経験は、AWS プラットフォームとインフラストラクチャに活かされています。AWS のデータセンターは、外部からはそれとはわからないようになっています。ビデオ監視カメラ、最新鋭の侵入検出システム、その他エレクトロニクスを使った手段を用いて、専門のセキュリティスタッフが、建物の入口とその周辺両方において、物理的アクセスを厳密に管理しています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行います。 AWS は、そのような権限に対して正規のビジネスニーズがある従業員や業者に対してのみデータセンターへのアクセスや情報を提供しています。従業員がこれらの特権を必要とする作業を完了したら、たとえかれらが引き続き Amazonまたは Amazon Web Services の従業員であったとしても、そのアクセス権は速やかに取り消されます。AWS 従業員によるデータセンターへのすべての物理的アクセスは記録され、定期的に監査されます。 詳細に関しては「セキュリティプロセスの概要（2014年11月）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf
7	7.1	7.1.2	(1)	(b)	情報システムセキュリティ責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、要安定情報を取り扱う情報システムについて、サービス提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保すること。	適合可能	・情報システムセキュリティ責任者は、システム導入・運用にあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウドを利用する場合には、以下に例示するように、Auto Scaling、マルチAZ（アベイラビリティゾーン）等を用いて可用性を確保する構成を考慮することが望ましい。 -AWSクラウドのAuto scalingサービスにて、ある閾値を超えた場合に仮想サーバを追加するといった機能にて過負荷を防ぐことができるため、これらの機能を利用する -冗長構成については、AWSクラウドのマルチAZ（アベイラビリティゾーン）での冗長構成を考慮する ・AWSクラウド自体においてサービスレベルアグリーメントにてサービス毎の商業的努力目標値を定めており、当該可用性についても考慮する必要がある。例)EC2：99.95% ・障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、要安定情報を取り扱う情報システムについて、以下に例示するように当該情報システムを構成する各サーバ（インスタンス）に求められる可用性要件を考慮することが望ましい。 - 負荷分散装置による負荷分散構成とすること - 同一システムを二系統で構成することにより冗長化すること	・AWSクラウドは、以下に示すような回復機能を持つ IT アーキテクチャを配備する機能を提供しており、これらを利用してシステムの可用性を実現することが可能。 - AWSのすべてのデータセンターはオンラインでサービスを提供し、「コールド」状態のデータセンターは存在しない。 -データセンター障害時には、自動プロセスにより、顧客データが影響を受けるエリアから移動される。 -データセンター障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在。 - AWSクラウドの各リージョンには複数のアベイラビリティゾーン（データセンターのこと。以下、AZとする。）が存在しており、AZは、地理、電源、ネットワーク的に分離され、各AZは高速専用線で接続される。 ・AWSクラウドは、複数のアベイラビリティゾーンにアプリケーションを配置することで、自然災害やシステム障害を含むほとんどの障害が発生したときに、回復力を持った状態を保つための機能を提供しており、これらを利用してシステムの可用性を実現することが可能。	可用性 世界各地に設置されているデータセンターは、所在地によりリージョンに分けられています。すべてのデータセンターはオンラインでお客様にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、顧客データが影響を受けるエリアから移動されます。重要なアプリケーションはN+1原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。 AWSを使用すると、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理上のリージョン内に、柔軟にインスタンスを配置してデータを保管できます。各アベイラビリティーゾーンは、障害が発生しても他のゾーンに影響を与えないように設計されています。つまり、アベイラビリティゾーンは、代表的な都市のリージョン内で物理的に区切られており、低リスクの氾濫原にあります（具体的な洪水帯の分類はリージョンによって異なります）。個別の無停電電源装置（UPS）やオンサイトのバックアップ生成施設に加え、シングルポイントの障害の可能性を減らすために、別々の電力供給施設から異なる配管網を経由して、個別に電力供給を行っています。アベイラビリティゾーンはすべて、複数のTier-1トランジットプロバイダに重複して接続しています。 AWSを利用する際には、複数のリージョンやアベイラビリティーゾーンを利用できるように設計することをお勧めします。複数のアベイラビリティゾーンにアプリケーションを配置すると、自然災害やシステム障害を含むほとんどの障害が発生したときに、回復力を持った状態を保つことができます。 詳細に関しては「セキュリティプロセスの概要（2014年11月）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf 高可用性および事業継続性の維持 AWSは、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。各アベイラビリティーゾーンは、独立した障害ゾーンとして設計されています。障害時には、自動プロセスが、顧客データを影響を受けるエリアから移動します。詳細についてはAWS SOC1 TypeIIレポートに記載されています。ISO27001基準の付録A、ドメイン11.2に詳細が記載されています。AWSは独立監査人によりISO27001規格に準拠している旨の審査と認証を受けています。 詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf
7	7.1	7.1.2	(1)	(c)	情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、サーバ装置で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。	対象外	・サーバ装置で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めるここについては、クラウドサービス利用有無にかかわらず情報システムセキュリティ責任者が検討するべき事項である。	・ソフトウェアの導入・運用については本リファレンスの説明の対象外。	−
7	7.1	7.1.2	(1)	(d)	情報システムセキュリティ責任者は、通信回線を経由してサーバ装置の保守作業を行う際に送受信される情報が漏えいすることを防止するための対策を講ずること。	適合可能	・情報システムセキュリティ責任者は、システム導入・運用にあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド利用時には、通信回線からの情報漏洩防止のため、AWSクラウドの提供するネットワークのセキュリティの仕組み（VPC、Direct Connect）の利用を検討することが望ましい。 ・通信回線を経由してサーバ装置の保守作業を行う際に送受信される情報について、以下に例示するように通信の暗号化に関する要件をを考慮することが望ましい。 - 秘匿要否 - 要秘匿の場合、情報の暗号化に係る要件	・AWSクラウドは、通信内容の秘匿を目的とし、情報をセキュアに送受信できるよう、以下の機能等を利用可能である。 - Amazon Virtual Private Cloud - AWS Direct Connect これらを利用し、通信回線を経由してサーバ装置の保守作業を行う際、情報をセキュアに送受信可能とする。	Amazon Virtual Private Cloud(Amazon VPC)では、アマゾン ウェブ サービス(AWS)クラウドの論理的に分離したセクションがプロビジョニングされ、ここからお客様が定義する仮想ネットワークでAWSリソースを起動できます。独自のIPアドレス範囲の選択、サブネットの作成、ルーティングテーブルとネットワークゲートウェイの設定など、仮想ネットワーク環境を完全にコントロールできます。 既存のデータセンターと自分のVPC間にハードウェア仮想プライベートネットワーク（VPN）接続を作成することができるので、AWSクラウドを既存のデータセンターを拡張するかのように活用することができます。 VPC 内のインスタンスへ、およびインスタンスからのすべてのトラフィックは、業界標準で暗号化された IPsec ハードウェア VPN 接続を通して、自社のデータセンターへルーティングすることができます。 詳細に関しては、https://aws.amazon.com/jp/vpc/ を参照してください。 また、AWS Direct Connectにより、お客様の設備からAWSへの専用ネットワーク接続を簡単に確立することができます。AWS Direct Connectを使用すると、AWSとデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。 詳細に関しては、https://aws.amazon.com/jp/directconnect/ を参照してください。 ネットワークの監視と保護 すべてのAWS APIは、サーバー認証を提供する、SSLで保護されたエンドポイント経由で利用可能です。 詳細に関しては「セキュリティプロセスの概要（2014年11月）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf
7	7.1	7.1.2	(2)	サーバ装置の運用時の対策					
7	7.1	7.1.2	(2)	(a)	情報システムセキュリティ責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。	対象外	・利用を認めるソフトウェア及び利用を禁止するソフトウェアの見直しを行うことは、クラウドサービス利用有無にかかわらず情報システムセキュリティ責任者が検討するべき事項である。	・利用を認めるソフトウェア及び利用を禁止するソフトウェアの見直しを行うことについては、本リファレンスの説明の対象外。	−

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
7	7.1	7.1.2	(2)	(b)	情報システムセキュリティ責任者は、所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、不適切な状態にあるサーバ装置を検出等した場合には改善を図ること。	適合可能	・AWSで取得しているSOC 1 Type II レポートでソフトウェアの変更管理に関するセキュリティ対策を確認の上、ユーザでAWSクラウドを利用して導入・運用する情報システムのセキュリティ対策を検討する。 [留意事項] ・AWSクラウドを利用する場合、システム構成やソフトウェアの状態を定期的に確認する情報の記録については、AWSクラウドの提供する機能(AWS Config)を利用することが望ましい。	・利用者は、AWSが変更管理に関し、既存の IT リソースに対する変更がある場合、当該内容が記録され、認証され、試験され、承認され、文書化されることについて合理的な保証を提供し統制目標として特定されていることについて、SOC 1 Type II レポートにて、独立監査人によって保証されていることを確認可能である。 ・AWSクラウドでは、AWS Config、Amazon Inspector、AWS Systems Manager、AWS Trusted Advisorを提供する。 -AWS Config…AWS リソースインベントリ、設定履歴、および設定変更通知といった機能を提供する。既存の AWS リソースと削除された AWS リソースの検出、ルールに対する全体的なコンプライアンスの判定、および任意の時点でのリソース設定の詳細な調査が可能。 -Amazon Inspector…自動化されたセキュリティ評価によって、アプリケーションのセキュリティ脆弱性やベストプラクティスからの逸脱を特定する機能を提供する。 -AWS Systems Manager…サービスの運用データ確認、AWS リソース全体に関わる運用タスクの自動化といった機能を提供する。システム設定やパッチレベル、ソフトウェアのインストール状況等の最新情報を確認することで、素早い問題特定が可能。 -AWS Trusted Advisor…ユーザーの AWS 環境を分析し、推奨ベストプラクティスを提供する。コスト削減、パフォーマンスの向上、セキュリティの向上に役立つオンラインリソース。	・アマゾン ウェブ サービスは現在、Service Organization Controls 1 (SOC 1)、Type II レポートを発行しています。 レポートには AWS SOC 1 の統制目標が記載されており、このレポート自体に、各統制目標と独立監査人による各統制のテスト手順の結果をサポートする統制活動が特定されています。 変更管理 ・統制は、既存の IT リソースに対する変更 (緊急/特殊な設定) が記録され、認証され、試験され、承認されて文書化されることについて、合理的な保証を提供するものです。 詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf ソフトウェア AWS は、変更の管理にシステム的なアプローチを採用しています。そのためお客様に影響を与えるサービスの変更は、徹底的に検証、テスト、承認され、充分な情報が提供されます。AWS の変更管理プロセスは、意図しないサービス障害を防ぎ、お客様に対するサービスの完全性を維持することを目的としています。実稼働環境にデプロイされる変更には、以下の対応が行われます: • 検証: 変更の技術的側面について専門家による検証が必要です。 • テスト: 適用されている変更は、予想どおりに動作し、パフォーマンスに悪影響を与えないことを確認するためにテストされます。 • 承認: すべての変更は、ビジネスへの影響を適切に監視し、それらの影響についての情報を提供するために、承認される必要があります。 詳細に関しては「セキュリティプロセスの概要（2014年11月）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf AWS Config は完全マネージド型のサービスで、セキュリティとガバナンスのため、AWS リソースインベントリ、設定履歴、および設定変更通知といった機能が用意されています。Config Rules を使用して、AWS Config によって記録された AWS リソース設定を自動的にチェックするルールを作成できます。 AWS Config を使用することで、既存の AWS リソースと削除された AWS リソースとの検出、ルールに対する全体的なコンプライアンスの判定、および任意の時点でのリソース設定の詳細な調査が可能になります。これらの機能は、コンプライアンス監査、セキュリティ分析、リソース変更の追跡、トラブルシューティングを可能にします。 詳細に関しては、https://aws.amazon.com/jp/config/ を参照してください。 Amazon InspectorはAWS にデプロイされたアプリケーションのセキュリティとコンプライアンスを向上させるための、自動化されたセキュリティ評価サービスです。自動的にアプリケーションを評価し、脆弱性やベストプラクティスからの逸脱がないかどうかを確認します。評価が実行された後、重大性の順にセキュリティの調査結果を示した詳細なリストが Amazon Inspector によって作成されます。 詳細に関しては、 https://aws.amazon.com/jp/inspector/ を参照してください。 AWS Systems Manager は、利用するインフラストラクチャを可視化し、制御するためのサービスです。Systems Manager を使用すると、統合ユーザーインターフェイスで AWS のさまざまなサービスの運用データを確認でき、AWS リソース全体に関わる運用タスクを自動化できます。これにより、さまざまなリソースグループのモニタリングやトラブルシューティングを迅速に行うことができ、リソースとアプリケーションの管理を簡素化することも可能です。運用上の問題の検出と解決に要する時間が短縮され、大規模なインフラストラクチャやでも安全に運用、管理できます。 詳細に関しては、 https://aws.amazon.com/jp/systems-manager/ を参照してください。 AWS Trusted Advisorは、AWS 環境を最適化することで、コスト削減、パフォーマンスの向上、セキュリティの向上に役立つオンラインリソースです。Trusted Advisor では、AWS ベストプラクティスに従ってリソースをプロビジョニングするのに役立つ、リアルタイムガイダンスを提供しています。 詳細に関しては、 https://aws.amazon.com/jp/premiumsupport/trustedadvisor/ を参照してください。
7	7.1	7.1.2	(2)	(c)	情報システムセキュリティ責任者は、サーバ装置上での不正な行為、無許可のアクセス等の意図しない事象の発生を検知する必要がある場合は、当該サーバ装置を監視するための措置を講ずること。ただし、サーバ装置の利用環境等から不要と判断できる場合はこの限りではない。	適合可能	・AWSクラウドにおけるインシデント応答については、AWSクラウド自身で管理する。これを踏まえて、情報システムセキュリティ責任者は、AWSクラウドを利用して情報システムを導入・運用するか否かについて判断する必要がある。また、AWSクラウドを利用して導入・運用する情報システムのセキュリティ対策を検討し対策を講ずることについては、ユーザ責任で実施する必要がある。 [留意事項] ・情報システムセキュリティ責任者は、以下に例示するように、サーバ装置上での不正な行為、無許可のアクセス等の意図しない事象の発生の検知及び当該サーバ装置を監視するための措置を定める必要があることに留意する。ただし、サーバ装置の利用環境等から不要と判断できる場合はこの限りではない。 - アクセスログ、エラーログ等を定期的に確認する。（AWSクラウド利用時には、ログ取得・管理のためにCloudTrailサービスの利用を検討することが望ましい。） - IDS/IPS、WAF等を設置する（AWSクラウド利用時には、AWS WAFサービスの利用を検討することが望ましい。） - 不正プログラム対策ソフトウェアを利用する - ファイル完全性チェックツールを利用する - CPU、メモリ、ディスクI/O等のシステム状態を確認する	・AWSクラウドは、AWSクラウドそのものに対するインシデント対応として、主要なメトリクスをモニタリングしており、しきい値を超えると、AWSインシデント対応プロセスが開始される。 ・AWS のインシデント管理プログラムは、SOC、PCI DSS、ISO 27001、および FedRAMP のコンプライアンスの監査時に、社外の独立監査人によって確認される。 ・AWSクラウドは、システムに対するアクセスログ等を取得し確認するための機能を提供する。（詳細は、「6.1.4 (1) ログの取得・管理」参照。 ・AWSクラウドは、機器等の脆弱性を悪用した不正な操作を防止する機能を持つAWS WAF （ウェブアプリケーションファイアウォール）を提供する。（詳細は、「7.2.4 (1) (d)」参照。） ・AWSクラウドは、悪意のある操作や不正な動作などの脅威を機械学習を用いて検出する機能を持つAmazon Guard Dutyを提供する。	セキュリティ組織 ・AWS 内のシステムには、運用とセキュリティの主要なメトリクスをモニタリングする膨大な装置が備わっています。主要なメトリクスが早期警告しきい値を超えた場合、運用管理担当者に自動的に通知されるよう、アラームが設定されています。しきい値を超えた場合、AWS インシデント対応プロセスが開始されます。Amazon のインシデント対応チームでは、業務に影響するイベントが発生した場合に解決を促進する、業界標準の診断手順を採用しています。スタッフは、24 時間年中無休体制でインシデントを検出し、解決への影響を管理します。 インシデントへの対応 ・AWS では、インシデント対応に関する文書化された正規のポリシーとプログラムを実施してきました。インシデント対応ポリシーでは、目的、範囲、役職、責任、および管理の取り組みについて扱っています。 ・AWS では、インシデントを管理するために 3 段階のアプローチを使用しています。 1. 対応開始/通知フェーズ: イベントの検出により、AWS のインシデントが開始されます。 イベントがインシデント基準を満たす場合、関係するオンコールサポートエンジニアが AWS イベント管理ツールシステムを使用して対応を開始し、関係するプログラムの担当者を呼び出します。担当者はインシデントの分析を実行し、別の担当者の対応が必要かどうかを判断して、おおまかな原因を特定します。 2. 復旧フェーズ: 関係する担当者が不具合の修正を実行して、インシデントに対応します。トラブルシューティング、不具合の修正、影響を受けたコンポーネントへの対応が実行されたなら、呼び出しを行ったリーダーはフォローアップの文書化やアクションのために次のステップを割り当て、呼び出し対応を終了します。 3. 再構成フェーズ: 関係する修正活動が完了したら、呼び出しを行ったリーダーは復旧フェーズの完了を宣言します。インシデントの事後検討と原因の詳細な分析が、関係するチームに割り当てられます。関係する上級管理職が事後検討の結果を確認します。設計の変更などの関係するアクションがエラー修正 (COE) ドキュメントに記録され、その実行が追跡されます。 ・AWS のインシデント管理プログラムは、SOC、PCI DSS、ISO 27001、および FedRAMP のコンプライアンスの監査時に、社外の独立監査人によって確認されます。 ・AWS のお客様の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、およびデータの所有権と制御はお客様が保持しているため、コンテンツ (データ) のワークフローの文書化はお客様の責任となります。 詳細に関しては、https://aws.amazon.com/jp/compliance/mpaa/ を参照してください。 Amazon GuardDuty は、AWS アカウントとワークロードを保護するために悪意のある操作や不正な動作を継続的にモニタリングする脅威検出サービスです。アカウント侵害の可能性を示す異常な API コールや不正なデプロイなどのアクティビティをモニタリングします。インスタンスへの侵入の可能性や攻撃者による偵察も検出します。 詳細に関しては、 https://aws.amazon.com/jp/guardduty/ を参照してください。

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
7	7.1	7.1.2	(2)	(d)	情報システムセキュリティ責任者は、要安定情報を取り扱うサーバ装置について、サーバ装置が運用できなくなった場合に正常な運用状態に復元することが可能となるよう、必要な措置を講ずること。	適合可能	・情報システムセキュリティ責任者は、システム導入・運用にあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウドを利用する場合には、Auto Scaling、マルチAZ（アベイラビリティゾーン）等を用いて可用性を確保する構成を考慮することが望ましい。 ・障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、要安定情報を取り扱う情報システムについて、以下に例示するように当該情報システムを構成する各サーバ（インスタンス）に求められる可用性要件を考慮することが望ましい。 - 負荷分散装置による負荷分散構成とすること - 同一システムを2系統で構成することにより冗長化すること ・AWSクラウドを利用する場合には、EC2スナップショットや、ストレージ上のデータのスナップショット等、AWSクラウドの機能を利用してバックアップ取得を実現することが望ましい。 ・情報システムセキュリティ責任者は、要安定情報を取り扱うサーバ装置について、サーバ装置が運用できなくなった場合に正常な運用状態に復元することが可能となるよう、以下に例示するようにバックアップ要件を定める必要があることに留意する。 - サーバの運用に必要なソフトウェアの原本を別に用意 - サービスの提供に必要なデータ、利用者が入力したデータ、システム設定等の定期的なバックアップ - サーバを冗長構成にしている場合、サーバの切替訓練を実施 - バックアップとして取得した情報から復元するための訓練を実施	・AWSクラウドは、以下に示すようなバックアップ等の機能を提供しており、これらを利用し、サーバ（インスタンス）について、サーバ（インスタンス）が運用できなくなった場合に正常な運用状態に復元することが可能。 -サーバインスタンスについては、EC2のスナップショットの取得が可能。 -ストレージサービス（S3、Glacier）の利用が可能であり、当該サービスでは、データが自動的に複数データセンター間でレプリケートされ、高い耐久性を実現（設計上の耐久性は 99.999999999%（イレブン・ナイン）） ・ディザスタリカバリを考慮した構成として、複数のアベイラビリティーゾーンを使った冗長構成（Multi-AZ）を可能とする。	可用性 AWSを利用する際には、複数のリージョンやアベイラビリティーゾーンを利用できるように設計することをお勧めします。複数のアベイラビリティゾーンにアプリケーションを配置すると、自然災害やシステム障害を含むほとんどの障害が発生したときに、回復力を持った状態を保つことができます。 データの堅牢性と信頼性 Amazon S3 は、任意の 1 年間について 99.999999999% のオブジェクト堅牢性を提供するよう設計されています。オブジェクトは、Amazon S3 のリージョン内の複数の施設の複数のデバイスで冗長的に格納されます。 Elastic Block Storage (Amazon EBS) セキュリティ Amazon EBS ボリュームに保存されるデータは、これらのサービスの通常オペレーションの一部として、複数の物理的ロケーションで冗長的に保存され、追加費用はかかりません。ただし、Amazon EBS のレプリケーションは、複数のアベイラビリティゾーンに分散されるのではなく、同一のアベイラビリティゾーン内に保存されます。そのため、長期的なデータ堅牢性を考えて、定期的に Amazon S3 にスナップショットを作成することを強くお勧めします。 AWS Storage Gateway のセキュリティ AWS Storage Gateway は、データを Amazon EBS スナップショット形式でオフサイトの Amazon S3 に透過的にバックアップします。Amazon S3 は複数の施設全体にある複数デバイス上のスナップショットを冗長に保存し、冗長性が失われれば検出し、修正します。Amazon EBS スナップショットは、オンプレミスで復元可能な、または新しいAmazon EBS ボリュームでインスタンス化するために使用するポイントインタイムバックアップを提供します。データは、指定する単一のリージョン内に保存されます。 詳細に関しては「セキュリティプロセスの概要（2014年11月）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf Amazon S3 と Amazon Glacier では、データが自動的に複数データセンター間でレプリケートされるので、高い耐久性を実現でき、設計上の耐久性は 99.999999999% となっています 詳細に関しては、https://aws.amazon.com/jp/backup-storage/ を参照してください。
7	7.1	7.1.2	(3)	サーバ装置の運用終了時の対策					
7	7.1	7.1.2	(3)	(a)	情報システムセキュリティ責任者は、サーバ装置の運用を終了する際に、サーバ装置の電磁的記録媒体の全ての情報を抹消すること。	適合可能	・AWSが取得しているISO27001の認証でAWSクラウドデータセンター内のサーバやストレージ等のハードウェアデバイスの廃棄やデータ消去に関するセキュリティ対策を確認の上、ユーザでAWSクラウドを利用して導入・運用する情報システムのセキュリティ対策を検討する。 [留意事項] ・AWSクラウドを利用する場合、削除した EBS ボリュームが使用していた物理的なブロックストレージは、別のアカウントに割り当てられる前に、ゼロで上書きされるが、機密情報を扱う場合は、別途データ暗号化を行っておき、システム運用終了時に暗号化のための鍵データを削除するといったデータ抹消相当の対応の必要があることに留意する。 ・情報システムセキュリティ責任者は、サーバ（インスタンス）の運用を終了する際に、情報の漏えいを防止するため、以下に例示するような対策を講じる必要があることに留意する。 - サーバ（インスタンス）の電磁的記録媒体の全ての情報を抹消する - データ抹消ソフトウェア（もとのデータに異なるランダムなデータを複数回上書きすることでデータを抹消する）によりファイルを抹消する - 保存されている情報の漏えいが生じないための対策を講じることを契約内容に含める	・AWSは、ISO27001に準拠して、ストレージデバイスが製品寿命に達した場合、以下いずれかに記載されている技術を用いて廃棄プロセスの一環としてデータを破棄しており、利用者は、これらの認証を取得していることを確認可能である。 - DoD5220.22-M - NIST800-88 また、ハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁又は物理的に破壊する。 ・削除した EBS ボリュームが使用していた物理的なブロックストレージは、別のアカウントに割り当てられる前に、ゼロで上書きされる。	AWSの処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWSは、DoD 5220.22-M（「National Industrial Security Program OperatingManual（国立産業セキュリティプログラム作業マニュアル）」）またはNIST 800-88（「Guidelines for Media Sanitization（メディア衛生のためのガイドライン）」）に詳細が記載されている技術を用いて、廃棄プロセスの一環としてデータを破棄します。廃棄された磁気ストレージデバイスはすべて業界標準の方法に従って消磁され、物理的に破壊されます。 詳細に関しては「セキュリティプロセスの概要（2014年11月）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf ISO27001基準に合わせて、AWSの処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWSはDoD5220.22-MまたはNIST800-88に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。 詳細については、ISO27001規格の附属書A、ドメイン9.2を参照してください。AWSは、ISO27001認定基準への対応を確認する独立監査人から、検証および認定を受けています。 詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf データの永続性 データは、ボリュームを明示的に削除するまでボリュームに保持されます。削除した EBS ボリュームが使用していた物理的なブロックストレージは、別のアカウントに割り当てられる前に、ゼロで上書きされます。機密データを扱っている場合は、手動によるデータの暗号化や、Amazon EBS 暗号化 で保護されているボリュームへのデータの格納を検討してください。詳細については、「Amazon EBS Encryption」を参照してください。 デフォルトでは、インスタンスの起動時に作成およびアタッチされた EBS ボリュームは、インスタンスの終了時に削除されます。この動作を変更するには、インスタンスの起動時にフラグ DeleteOnTermination の値を false に変更します。値を変更すると、インスタンスが終了してもボリュームが保持されるので、そのボリュームを別のインスタンスにアタッチできます。 詳細に関しては、http://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSVolumes.html を参照してください。 13. AWS Import/Export 13.14 アプライアンスの外的状況にかかわらず、また、サービス利用者が、アプライアンスが損傷しているまたは機能していない可能性があると考える場合であっても、サービス利用者はアマゾンに対して、全てのアプライアンスを返却するものとする。アプライアンスは廃電気・電子機器ではなく、また、サービス利用者はアプライアンスの最終ユーザーとはならないが、疑義を避けるために付言すると、サービス利用者は、アプライアンスが廃電気・電子機器として（未分類市町村廃棄物とされる場合を含む）、またはその他の廃棄物収集過程において処分されるものではないこと、本契約の条項に従ったサービス利用者による使用されたアプライアンスのアマゾンへの返却が、アプライアンスの耐用年数の延長およびアプライアンスが耐用年数に達したときのアマゾンによるその責任ある取扱およびリサイクルに貢献すること、また、その他の電子・電気機器と同様、かかる機器における有害物質の存在の結果、アプライアンスの処分または不適切な取扱が、環境および人の健康に悪影響を与える可能性があることを了解するものとする。疑義を避けるために述べると、本項の条件はアプライアンスに含まれる内蔵バッテリーにも適用される。サービス利用者は、アプライアンスの内蔵バッテリーにアクセスしまたはこれを移動もしくは移転してはならない。アプライアンスは、かかる要件を反映するため、および一定の管轄地域における廃棄物関連の規制要件に従って、クロスドアウト・ホイール・ピンのシンボルマークが付されている。 詳細に関しては、https://aws.amazon.com/jp/service-terms/ を参照してください。
7	7.1	7.1.3	複合機・特定用途機器						
7	7.1	7.1.3	(1)	複合機					
7	7.1	7.1.3	(1)	(a)	情報システムセキュリティ責任者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、適切なセキュリティ要件を策定すること。	対象外			-
7	7.1	7.1.3	(1)	(b)	情報システムセキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講ずること。	対象外			-
7	7.1	7.1.3	(1)	(c)	情報システムセキュリティ責任者は、複合機の運用を終了する際に、複合機の電磁的記録媒体の全ての情報を抹消すること。	対象外			-
7	7.1	7.1.3	(2)	IoT 機器を含む特定用途機器					
7	7.1	7.1.3	(2)	(a)	情報システムセキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じた対策を講ずること。	対象外			-

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
7	7.2	電子メール・ウェブ等							
7	7.2	7.2.1	電子メール						
7	7.2	7.2.1	(1)	電子メールの導入時の対策					
7	7.2	7.2.1	(1)	(a)	情報システムセキュリティ責任者は、電子メールサーバが電子メールの不正な中継を行わないように設定すること。	対象外			−
7	7.2	7.2.1	(1)	(b)	情報システムセキュリティ責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に主体認証を行う機能を備えること。	対象外			−
7	7.2	7.2.1	(1)	(c)	情報システムセキュリティ責任者は、電子メールのなりすましの防止策を講ずること。	対象外			−
7	7.2	7.2.1	(1)	(d)	情報システムセキュリティ責任者は、インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、電子メールのサーバ間通信の暗号化の対策を講ずること。	対象外			
7	7.2	7.2.2	ウェブ						
7	7.2	7.2.2	(1)	ウェブサーバの導入・運用時の対策					
7	7.2	7.2.2	(1)	(a)	情報システムセキュリティ責任者は、ウェブサーバの管理や設定において、以下の事項を含む情報セキュリティ確保のための対策を講ずること。		(ア)から(オ)に対応する以下の記載を参照のこと。	(ア)から(オ)に対応する以下の記載を参照のこと。	−
7	7.2	7.2.2	(1)	(a)	(ア) ウェブサーバが備える機能のうち、不要な機能を停止又は制限すること。	適合可能	・情報システムセキュリティ責任者は、Webサーバ導入・運用にあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド利用時には、AWSクラウドの提供するインフラストラクチャ自体が標準で設定されている要塞化（最小権限の実装等）を踏まえたうえで、要塞化（例：利用しないサービスやポートの停止、利用しないテストアカウントの削除や、SSHやRDPなどサーバ管理を行うサービスについては、ウェルノウンポートを利用しない等）を検討することが望ましい。	・AWSクラウドの提供するインフラストラクチャは以下に示すような実装をしており、これらによりサーバインスタンスの要塞化が可能。 -最小権限を実装。 -特定のビジネス目的を持っていないすべてのポートとプロトコルを禁止 -定期的な内外部の脆弱性のスキャンを実行。	インフラストラクチャおよび仮想化セキュリティ OS のセキュリティ強化とベースコントロール（IVS-07.1） ・AWS ネットワーク管理は、SOC、PCI DSS、ISO 27001、および FedRAMP への AWS の継続的な準拠の一環として、第三者の独立監査人によって定期的に確認されます。 ・AWS は、そのインフラストラクチャコンポーネントを通じて最小権限を実装しています。また、特定のビジネス目的を持っていないすべてのポートとプロトコルを禁止しています。AWS は、デバイスの使用に不可欠な機能のみの最小実装という厳格な手法に従っています。ネットワークスキャンを実行し、不要なポートまたはプロトコルが使用されている場合は修正されます。 ・AWS 環境内のホストオペレーティングシステム、ウェブアプリケーション、およびデータベースできまざまなツールを利用した、定期的な内外部の脆弱性のスキャンが実行されます。脆弱性のスキャンと解決手法は、AWS の PCI DSS および FedRAMP への継続的な準拠の一環として定期的に確認されます。 詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf
7	7.2	7.2.2	(1)	(a)	(イ) ウェブコンテンツの編集作業を担当する主体を限定すること。	適合可能	・情報システムセキュリティ責任者は、Webサーバ導入・運用にあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド利用時には、AWS IAMを利用し、サービス/リソースへのアクセスコントロールを実現することが望ましい。但し、AWS IAMは、AWSの提供するAWSクラウド上で構築するアプリケーションへのアクセスコントロールについては提供しないことに留意する。 ・ウェブコンテンツデータに対するアクセス権限設定や、不要な識別コードを削除すること等について、AWSクラウド利用の無い従来の情報システムと同様に検討する必要があることに留意する。	・AWSクラウドは、アクセス権を使用して AWS リソースへのアクセスを許可および拒否できる仕組み（AWS IAM機能）提供している。これを利用し、アクセスできるユーザーを制御することが可能。(詳細は、「6.1.1 主体認証機能」、「6.1.2 アクセス制御機能」を参照。)	AWS Identity and Access Management (IAM) により、お客様のユーザーの AWS サービスおよびリソースへのアクセスを安全にコントロールすることができます。IAM を使用すると、AWS のユーザーとグループを作成および管理し、アクセス権を使用して AWS リソースへのアクセスを許可および拒否できます。 詳細に関しては、https://aws.amazon.com/jp/iam/ を参照してください。
7	7.2	7.2.2	(1)	(a)	(ウ) 公開してはならない又は無意味なウェブコンテンツが公開されないように管理すること。	対象外	・公開を想定していないファイルを公開ディレクトリに置かないこと、不要なコンテンツやサンプルページを削除すること等、公開してはならない又は無意味なウェブコンテンツが公開されないように管理することについて、クラウドサービス利用有無にかかわらず情報システムセキュリティ責任者が検討するべき事項である。	・ウェブコンテンツの公開に関する管理については、本リファレンスの説明の対象外。	−
7	7.2	7.2.2	(1)	(a)	(エ) ウェブコンテンツの編集作業に用いる端末を限定し、識別コード及び主体認証情報を適切に管理すること。	適合可能	・情報システムセキュリティ責任者は、Webサーバ導入・運用にあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド利用時には、セキュリティグループを用い、ウェブコンテンツの編集作業等の運用時のアクセスについて、指定IP以外からのアクセスを許可しない設定が可能。ただし、物理的な端末の限定を行うものではないため、端末の限定そのものは、運用ルールまたは運用作業をする執務環境側で検討する必要があることに留意する。	・AWSクラウドの提供するセキュリティグループ設定にて、各サーバインスタンスに許可する通信制御を行うことが可能。	セキュリティグループ ・セキュリティグループを使用して、お客様の Amazon EC2 インスタンスにアクセスするためのプロトコル、ポート、およびソース IP アドレス範囲を制御できます。つまり、これはお客様のインスタンスのファイアウォールルールを定義するものです。 詳細に関しては「セキュリティプロセスの概要（2014年11月）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf ・セキュリティグループは、インスタンスの仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィックをコントロールします。VPC 内でインスタンスを起動した場合、そのインスタンスは最大 5 つのセキュリティグループに割り当てることができます。セキュリティグループは、サブネットレベルでなくインスタンスレベルで動作します。このため、VPC 内のサブネット内のインスタンスごとに異なるセキュリティグループのセットに割り当てることができます。起動時に特定のグループを指定しないと、インスタンスは VPC のデフォルトのセキュリティグループに自動的に割り当てられます。 ・セキュリティグループごとに、インスタンスへのインバウンドトラフィックをコントロールするルールと、アウトバウンドトラフィックをコントロールする一連のルールを個別に追加します。 詳細に関しては、http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html を参照してください。

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
7	7.2	7.2.2	(1)	(a)	(オ) インターネットを介して転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講じること。	適合可能	・情報システムセキュリティ責任者は、Webサーバ導入・運用にあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド利用時には、通信の暗号化を行う必要がある場合、IPSec VPN接続、Direct Connectの利用や、AWSクラウドのELB（Elastic Load Balancing）にてHTTPS (SSL or TLS) の使用を検討することが望ましい。 ・AWSクラウドのELBを利用する場合、ELBに TLS（SSL） 証明書をデプロイする必要があることを考慮すること。 ・通信の暗号化やサーバ証明を行う際、以下の点に留意すること。 -TLS（SSL）機能のために必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いる -暗号技術検討会及び関連委員会（CRYPTREC）により作成された「SSL/TLS暗号設定ガイドライン」に従って、TLS（SSL）サーバを適切に設定する。 -SSL プロトコルには、通信の一部が第三者に解読可能な脆弱性が存在するためTLSを利用する	・AWSクラウドは、以下の機能を提供しており、これらを利用し、通信の盗聴や情報漏洩を防止するための通信の暗号化が可能。 -IPSec ハードウェアVPN接続…業界標準で暗号化されたAWSクラウド上のインスタンスに対する接続を提供。 -AWS Direct Connect…ユーザの設備からAWSへの専用ネットワーク接続を提供。 -Webサーバへのロードバランシングとしてサービスの ELB(Elastic Load Balancing）を利用する場合、クライアントとELB間の通信についてSSL/TLS による暗号化（HTTPS通信）の仕組みを提供。	・Amazon Virtual Private Cloud(Amazon VPC)では、アマゾン ウェブ サービス(AWS)クラウドの論理的に分離したセクションがプロビジョニングされ、ここからお客様が定義する仮想ネットワークでAWSリソースを起動できます。独自のIPアドレス範囲の選択、サブネットの作成、ルーティングテーブルとネットワークゲートウェイの設定など、仮想ネットワーク環境を完全にコントロールできます。 ・VPC 内のインスタンスへ、およびインスタンスからのすべてのトラフィックは、業界標準で暗号化された IPsec ハードウェア VPN 接続を通して、自社のデータセンターへルーティングすることができます。 詳細に関しては、https://aws.amazon.com/jp/vpc/ を参照してください。 ・AWS Direct Connectにより、お客様の設備からAWSへの専用ネットワーク接続を簡単に確立することができます。AWS Direct Connectを使用すると、AWSとデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。 詳細に関しては、https://aws.amazon.com/jp/directconnect/ を参照してください。 ・Elastic Load Balancing は、証明書管理および SSL 復号を統合し、ロードバランサーの SSL 設定を集中管理し、CPU に負荷のかかる作業をインスタンスから切り離すことができます。Elastic Load Balancing は、AWS Certificate Manager と統合することにより、サイトやアプリケーションに対して簡単に SSL/TLS を有効化することも可能です。証明書管理、マネージド型の証明書更新とデプロイ、および SSL/TLS 復号が統合できるため、ロードバランサーの SSL/TLS 設定を一括で管理できます。 詳細に関しては、https://aws.amazon.com/jp/elasticloadbalancing/ を参照してください。
7	7.2	7.2.2	(1)	(b)	情報システムセキュリティ責任者は、ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認すること。	対象外	・ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認することについては、クラウドサービス利用有無にかかわらず情報システムセキュリティ責任者が検討するべき事項である。	・ウェブサーバに保存する情報の管理については、本リファレンスの説明の対象外。	-
7	7.2	7.2.2	(2)	ウェブアプリケーションの開発時・運用時の対策					
7	7.2	7.2.2	(2)	(a)	情報システムセキュリティ責任者は、ウェブアプリケーションの開発において、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講ずること。また、運用時においても、これらの対策に漏れが無いか定期的に確認し、対策に漏れがある状態が確認された場合は対処を行うこと。	対象外	・ウェブアプリケーションの脆弱性を排除するための対策を講ずること、また、運用時においても、これらの対策に漏れが無いか定期的に確認し、対策に漏れがある状態が確認された場合は対処を行うことについては、クラウドサービス利用有無にかかわらず情報システムセキュリティ責任者が検討するべき事項である。	・ウェブアプリケーションの開発・運用については、本リファレンスの説明の対象外。	-
7	7.2	7.2.3	ドメインネームシステム（DNS）						
7	7.2	7.2.3	(1)	DNS の導入時の対策					
7	7.2	7.2.3	(1)	(a)	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムの名前解決を提供するコンテンツサーバにおいて、名前解決を停止させないための措置を講ずること。	適合可能	・名前解決を停止させないための対処として、AWS の提供するDNSサービス（Amazon Route 53）の機能や特徴を踏まえ、サービス利用を検討することが必要。 ・情報システムセキュリティ責任者は、DNSサーバ導入・運用にあたり、独自にDNS機能を構築する場合、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド利用時には、AWSクラウドのDNSサービス（Amazon Route 53）は外部向けDNSだけでなく、AWS内部のDNS（Private DNS）としてDNSサービスを利用することが望ましい。また、オンプレミスや他ホスティングシステムのDNSを登録することも可能であることに留意する。 ・オンプレミスのネットワークとAWS VPC(Virtual Private Cloud)環境とのハイブリッドシステムを構築する場合、利用環境などに応じてDNSの設置場所などを検討する必要があることに留意する。	・AWSクラウドは、DNSサービス（Amazon Route 53）を提供し、このDNSサービスを、100%の使用可能時間の割合で使用（お客様の DNS クエリ応答に失敗しなかったこと）できるようにするため商業的に合理的な努力を行う。 このサービスを利用し、上記の範囲内で、機能を停止させずに名前解決機能を利用することが可能。	Amazon Route 53は、可用性と拡張性に優れたクラウドドメインネームシステム（DNS）ウェブサービスです。 DNS データをパブリックインターネットに公開することなく、内部 AWS リソースのカスタムドメイン名を管理します。 Amazon Route 53 は、AWS の高い可用性と信頼性を備えるインフラストラクチャを使用して構築されています。DNS サーバーの分散された性質により、お客様のエンドユーザーを確実にアプリケーションに転送します。Amazon Route 53 トラフィックフローなどの機能を使用すると、フェイルオーバーを簡単に設定して、プライマリのアプリケーションエンドポイントが利用できなくなった場合にユーザーを代替場所に再ルーティングできるため、信頼性が向上します。 詳細に関しては、https://aws.amazon.com/jp/route53/ を参照してください。 AWSは、Amazon Route 53を、100%の使用可能時間の割合で使用できるようにするため商業的に合理的な努力をします。 「100%の使用可能時間の割合」は、毎月の請求期間の間に Amazon Route 53 がお客様の DNS クエリ応答に失敗しなかったということを意味する。 詳細に関しては、https://aws.amazon.com/jp/route53/sla/ を参照してください。
7	7.2	7.2.3	(1)	(b)	情報システムセキュリティ責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答をするための措置を講ずること。	適合可能	・名前解決の要求への適切な応答のための対処として、AWS の提供するDNSサービス（Amazon Route 53）の機能や特徴を踏まえ、サービス利用を検討することが必要。 ・情報システムセキュリティ責任者は、DNSサーバ導入・運用にあたり、独自にDNS機能を構築する場合、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド利用時には、AWSクラウドのDNSサービス（Amazon Route 53）は外部向けDNSだけでなく、AWS内部のDNS（Private DNS）としてDNSサービスを利用することが望ましい。 ・Amazon Route 53 は DNSSEC for DNS をサポートしていないが、DNSSEC のドメイン登録は許可されていることに留意する。 ・オンプレミスのネットワークとAWS VPC(Virtual Private Cloud)環境とのハイブリッドシステムを構築する場合、利用環境などに応じてDNSの設置場所などを検討する必要があることに留意する。 ・独自にキャッシュサーバを構築する場合は、必要な要求にのみ応答する様、アクセス制御やファイアウォール等による制御を行うことを考慮することが望ましい。 ・独自にキャッシュサーバを構築する場合は、DNSキャッシュポイズニング攻撃から保護する為、ソースポートランダマイゼーション機能の導入やDNSSECの利用を考慮することが望ましい。	・AWSクラウドは、DNSサービス（Amazon Route 53）を提供し、このDNSサービスを、100%の使用可能時間の割合で使用（お客様の DNS クエリ応答に失敗しなかったこと）できるようにするため商業的に合理的な努力を行う。 このサービスを利用し、上記の範囲内で、適切な応答を実現する名前解決機能を利用することが可能。	Amazon Route 53は、可用性と拡張性に優れたクラウドドメインネームシステム（DNS）ウェブサービスです。 DNS データをパブリックインターネットに公開することなく、内部 AWS リソースのカスタムドメイン名を管理します。 Amazon Route 53 は、AWS の高い可用性と信頼性を備えるインフラストラクチャを使用して構築されています。DNS サーバーの分散された性質により、お客様のエンドユーザーを確実にアプリケーションに転送します。Amazon Route 53 トラフィックフローなどの機能を使用すると、フェイルオーバーを簡単に設定して、プライマリのアプリケーションエンドポイントが利用できなくなった場合にユーザーを代替場所に再ルーティングできるため、信頼性が向上します。 詳細に関しては、https://aws.amazon.com/jp/route53/ を参照してください。 AWSは、Amazon Route 53を、100%の使用可能時間の割合で使用できるようにするため商業的に合理的な努力をします。 「100%の使用可能時間の割合」は、毎月の請求期間の間に Amazon Route 53 がお客様の DNS クエリ応答に失敗しなかったということを意味する。 詳細に関しては、https://aws.amazon.com/jp/route53/sla/ を参照してください。 現時点では、Amazon Route 53 の DNS サービスは DNSSEC をサポートしていません。しかし、ドメイン名の登録サービスは、DNS サービスが別のプロバイダで構成される場合、署名されたドメイン用の DNSSEC キーの構成をサポートしています。ドメイン名登録向けの DNSSEC の構成の詳細については、こちら(http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/domain-configure-dnssec.html)をご覧ください。 詳細に関しては、https://aws.amazon.com/jp/route53/faqs/ を参照してください。

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
7	7.2	7.2.3	(1)	(c)	情報システムセキュリティ責任者は、コンテンツサーバにおいて、機関等のみで使用する名前の解決を提供する場合、当該コンテンツサーバで管理する情報が外部に漏えいしないための措置を講ずること。	適合可能	・名前解決を管理する情報が外部に漏えいしないための措置として、AWSの提供するDNSサービス（Amazon Route 53）の機能や特徴を踏まえ、サービス利用を検討することが必要。 ・情報システムセキュリティ責任者は、DNSサーバ導入・運用にあたり、独自にDNS機能を構築する場合、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWS内部のDNS（Private DNS）としてDNSサービスを利用することで、オンプレミスや他ホスティングシステムのDNSを登録することも可能であるが、AWSクラウドとの間のネットワークアクセスが必要であることに留意する。 ・Amazon Route 53 のアクセス権限に加えて、Amazon EC2 のアクセス権限を IAM に付与し、アクセス制御することを検討する必要があることに留意する。(IAMの詳細は、「6.1.1 主体認証機能」、「6.1.2 アクセス制御機能」を参照。) ・オンプレミスのネットワークとAWS VPC(Virtual Private Cloud)環境とのハイブリッドシステムを構築する場合、利用環境などに応じてDNSの設置場所などを検討する必要があることに留意する。	・AWSクラウドは、DNSサービス（Amazon Route 53）を提供し、このDNSサービスを、100%の使用可能時間の割合で使用（お客様の DNS クエリ応答に失敗しなかったこと）できるようにするため商業的に合理的な努力を行う。 このサービスを利用し、上記の範囲内で、コンテンツサーバで管理する情報が外部に漏えいしない名前解決機能を利用することが可能。	Amazon Route 53は、可用性と拡張性に優れたクラウドドメインネームシステム（DNS）ウェブサービスです。 DNS データをパブリックインターネットに公開することなく、内部 AWS リソースのカスタムドメイン名を管理します。 Amazon Route 53 は、AWS の高い可用性と信頼性を備えるインフラストラクチャを使用して構築されています。DNS サーバーの分散された性質により、お客様のエンドユーザーを確実にアプリケーションに転送します。Amazon Route 53 トラフィックフローなどの機能を使用すると、フェイルオーバーを簡単に設定して、プライマリのアプリケーションエンドポイントが利用できなくなった場合にユーザーを代替場所に再ルーティングできるため、信頼性が向上します。 詳細に関しては、https://aws.amazon.com/jp/route53/ を参照してください。 AWSは、Amazon Route 53を、100%の使用可能時間の割合で使用できるようにするため商業的に合理的な努力をします。 詳細に関しては、https://aws.amazon.com/jp/route53/sla/ を参照してください。 プライベートホストゾーンは、1 つ以上の Amazon Virtual Private Cloud (Amazon VPC) 内のドメインとそのサブドメインにトラフィックをルーティングする方法に関する情報を保持するコンテナです。 プライベートホストゾーンを作成するには、Amazon Route 53 アクションのアクセス権限に加えて、Amazon EC2 アクションのアクセス権限を IAM に付与する必要があります。 詳細に関しては、http://docs.aws.amazon.com/ja_jp/Route53/latest/DeveloperGuide/hosted-zones-private.html を参照してください。
7	7.2	7.2.3	(2)	DNS の運用時の対策					
7	7.2	7.2.3	(2)	(a)	情報システムセキュリティ責任者は、コンテンツサーバを複数台設置する場合は、管理するドメインに関する情報についてサーバ間で整合性を維持すること。	適合可能	・管理するドメインに関する情報についてサーバ間で整合性を維持するための対処として、AWS の提供するDNSサービス（Amazon Route 53）の機能や特徴を踏まえ、サービス利用を検討することが必要。 ・情報システムセキュリティ責任者は、DNSサーバ導入・運用にあたり、独自にDNS機能を構築する場合、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド利用時には、AWSクラウドのDNSサービス（Amazon Route 53）は外部向けDNSだけでなく、AWS内部のDNS（Private DNS）としてDNSサービスを利用することが望ましい。 ・オンプレミスのネットワークとAWS VPC(Virtual Private Cloud)環境とのハイブリッドシステムを構築する場合、利用環境などに応じてDNSの設置場所などを検討する必要があることに留意する。	・AWSクラウドは、DNSサービス（Amazon Route 53）を提供し、このDNSサービスを、100%の使用可能時間の割合で使用（お客様の DNS クエリ応答に失敗しなかったこと）できるようにするため商業的に合理的な努力を行う。 このサービスを利用し、上記の範囲内で、整合性を維持される名前解決機能を利用することが可能。	Amazon Route 53は、可用性と拡張性に優れたクラウドドメインネームシステム（DNS）ウェブサービスです。 詳細に関しては、https://aws.amazon.com/jp/route53/ を参照してください。 AWSは、Amazon Route 53を、100%の使用可能時間の割合で使用できるようにするため商業的に合理的な努力をします。 「100%の使用可能時間の割合」は、毎月の請求期間の間に Amazon Route 53 がお客様の DNS クエリ応答に失敗しなかったということを意味する。 詳細に関しては、https://aws.amazon.com/jp/route53/sla/ を参照してください。
7	7.2	7.2.3	(2)	(b)	情報システムセキュリティ責任者は、コンテンツサーバにおいて管理するドメインに関する情報が正確であることを定期的に確認すること。	適合可能	・管理するドメインに関する情報についてサーバ間で整合性を維持するための対処として、AWS の提供するDNSサービス（Amazon Route 53）の機能や特徴を踏まえ、サービス利用を検討することが必要。 ・情報システムセキュリティ責任者は、DNSサーバ導入・運用にあたり、独自にDNS機能を構築する場合、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド利用時には、AWSクラウドのDNSサービス（Amazon Route 53）は外部向けDNSだけでなく、AWS内部のDNS（Private DNS）としてDNSサービスを利用することが望ましい。 ・オンプレミスのネットワークとAWS VPC(Virtual Private Cloud)環境とのハイブリッドシステムを構築する場合、利用環境などに応じてDNSの設置場所などを検討する必要があることに留意する。	・AWSクラウドは、DNSサービス（Amazon Route 53）を提供し、このDNSサービスを、100%の使用可能時間の割合で使用（お客様の DNS クエリ応答に失敗しなかったこと）できるようにするため商業的に合理的な努力を行う。 このサービスを利用し、上記の範囲内で、管理するドメインに関する情報が正確な名前解決機能を利用することが可能。	Amazon Route 53は、可用性と拡張性に優れたクラウドドメインネームシステム（DNS）ウェブサービスです。 詳細に関しては、https://aws.amazon.com/jp/route53/ を参照してください。 AWSは、Amazon Route 53を、100%の使用可能時間の割合で使用できるようにするため商業的に合理的な努力をします。 「100%の使用可能時間の割合」は、毎月の請求期間の間に Amazon Route 53 がお客様の DNS クエリ応答に失敗しなかったということを意味する。 詳細に関しては、https://aws.amazon.com/jp/route53/sla/ を参照してください。
7	7.2	7.2.3	(2)	(c)	情報システムセキュリティ責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答を維持するための措置を講ずること。	適合可能	・管理するドメインに関する情報についてサーバ間で整合性を維持するための対処として、AWS の提供するDNSサービス（Amazon Route 53）の機能や特徴を踏まえ、サービス利用を検討することが必要。 ・情報システムセキュリティ責任者は、DNSサーバ導入・運用にあたり、独自にDNS機能を構築する場合、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド利用時には、AWSクラウドのDNSサービス（Amazon Route 53）は外部向けDNSだけでなく、AWS内部のDNS（Private DNS）としてDNSサービスを利用することが望ましい。 ・オンプレミスのネットワークとAWS VPC(Virtual Private Cloud)環境とのハイブリッドシステムを構築する場合、利用環境などに応じてDNSの設置場所などを検討する必要があることに留意する。	・AWSクラウドは、DNSサービス（Amazon Route 53）を提供し、このDNSサービスを、100%の使用可能時間の割合で使用（お客様の DNS クエリ応答に失敗しなかったこと）できるようにするため商業的に合理的な努力を行う。 このサービスを利用し、上記の範囲内で、適切な応答を維持する名前解決機能を利用することが可能。	Amazon Route 53は、可用性と拡張性に優れたクラウドドメインネームシステム（DNS）ウェブサービスです。 詳細に関しては、https://aws.amazon.com/jp/route53/ を参照してください。 AWSは、Amazon Route 53を、100%の使用可能時間の割合で使用できるようにするため商業的に合理的な努力をします。 「100%の使用可能時間の割合」は、毎月の請求期間の間に Amazon Route 53 がお客様の DNS クエリ応答に失敗しなかったということを意味する。 詳細に関しては、https://aws.amazon.com/jp/route53/sla/ を参照してください。
7	7.2	7.2.4	データベース						
7	7.2	7.2.4	(1)	データベースの導入・運用時の対策					

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
7	7.2	7.2.4	(1)	(a)	情報システムセキュリティ責任者は、データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行うこと。	適合可能	・情報システムセキュリティ責任者は、データベースサーバ導入・運用にあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSの提供するDBサービス（Amazon RDS）を使う場合、DB セキュリティグループは、VPC 内にない DB インスタンスへのネットワークアクセスを制御可能（これにより、APサーバとDBサーバを別VPCとし、APサーバからのIPアドレスのみ許可するという制御が可能）であり、これらの機能を踏まえた構成を考慮する必要がある。 ・Amazon RDSサービスを利用して構築するデータベースサーバに対するセキュリティを確保する対策は原則ユーザの責任において実施する必要がある。	・AWSクラウドは、Amazon RDSサービスとしてデータベース機能（Amazon Aurora、Oracle、Microsoft SQL Server、PostgreSQL、MySQL、MariaDB）をサービス提供しており、データベース機能を利用可能。 ・AWS IAM を使用してユーザーとアクセス許可を定義し、RDS データベースにアクセスできるユーザーを制御することが可能。(詳細は、「6.1.1 主体認証機能」、「6.1.2 アクセス制御機能」を参照。)	・Amazon Relational Database Service (Amazon RDS) は、クラウド上でリレーショナルデータベースを簡単にセットアップ、運用、拡大/縮小できるウェブサービスです。業界標準のリレーショナルデータベース向けに、費用対効果に優れた拡張機能を備え、一般的なデータベース管理タスクを管理します。 ・MySQL、MariaDB、PostgreSQL、Oracle、Microsoft SQL Server などの使い慣れたデータベース製品のほか、MySQL と互換性のある新しい Amazon Aurora DB エンジンを使用できます (詳細は「Amazon RDS での Aurora（http://docs.aws.amazon.com/ja_jp/AmazonRDS/latest/UserGuide/CHAP_Aurora.html)」を参照)。 ・データベースパッケージのセキュリティに加え、AWS IAM を使用してユーザーとアクセス許可を定義すると、RDS データベースにアクセスできるユーザーを制御するのに役立ちます。また、Virtual Private Cloud に配置すると、データベースを保護することもできます。 詳細に関しては、http://docs.aws.amazon.com/ja_jp/AmazonRDS/latest/UserGuide/Welcome.html を参照してください。
7	7.2	7.2.4	(1)	(b)	情報システムセキュリティ責任者は、データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずること。	適合可能	・情報システムセキュリティ責任者は、データベースサーバ導入・運用にあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSの提供するDBサービス（Amazon RDS）を使う場合、アクセスログの取得・管理のため、AWSクラウドの提供するCloudTrailサービスの利用を合わせて検討することが望ましい。ただし、CloudTrailは、AWSの提供するリソースへのリクエストを対象とするログを提供し、OS、アプリケーションやカスタムのログファイルについて自動的にログ取得/保管は行わない。 ・AWS上に構築可能なログ管理サービスを利用することが可能であるが、当該ログ管理サービスにどのようなログを取得するかなどについては、AWSクラウド利用の無い従来の情報システムと同様の検討をする必要がある。	・AWSクラウドは、システムに対するアクセスログ等を取得し確認するための機能を提供しており、ログの取得・確認を行うことが可能。（詳細は、「6.1.4 (1) ログの取得・管理」参照。 ・AWS上に構築可能なログ管理サービスを利用し、アプリケーション経由で、誰が、どのデータにアクセスしたかのログを記録/保管することが可能。	・Amazon Relational Database Service (Amazon RDS) は、クラウド上でリレーショナルデータベースを簡単にセットアップ、運用、拡大/縮小できるウェブサービスです。業界標準のリレーショナルデータベース向けに、費用対効果に優れた拡張機能を備え、一般的なデータベース管理タスクを管理します。 ・MySQL、MariaDB、PostgreSQL、Oracle、Microsoft SQL Server などの使い慣れたデータベース製品のほか、MySQL と互換性のある新しい Amazon Aurora DB エンジンを使用できます (詳細は「Amazon RDS での Aurora（http://docs.aws.amazon.com/ja_jp/AmazonRDS/latest/UserGuide/CHAP_Aurora.html)」を参照)。 ・データベースパッケージのセキュリティに加え、AWS IAM を使用してユーザーとアクセス許可を定義すると、RDS データベースにアクセスできるユーザーを制御するのに役立ちます。また、Virtual Private Cloud に配置すると、データベースを保護することもできます。 詳細に関しては、http://docs.aws.amazon.com/ja_jp/AmazonRDS/latest/UserGuide/Welcome.html を参照してください。
7	7.2	7.2.4	(1)	(c)	情報システムセキュリティ責任者は、データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講ずること。	適合可能	・情報システムセキュリティ責任者は、データベースサーバ導入・運用にあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSの提供するDBサービス（Amazon RDS）を使う場合、AWS上に構築可能なログ管理サービスを利用し、だれがいつどのような操作をしたかについて記録し、ある閾値以上などの条件かで警告を発する設定をすることについて検討する必要がある。その際、どのようなログを取得するかやどのような条件で警告とするかなどについては、AWSクラウド利用の無い従来の情報システムと同様の検討をする必要がある。 ・事務を遂行するに当たって不必要なデータの操作を検知できるよう、以下を例とする措置を講ずる検討（設計、構築、運用等）を行う必要がある。 a) 一定数以上のデータの取得に関するログを記録し、警告を発する。 b) データを取得した時刻が不自然であるなど、通常の業務によるデータベースの 操作から逸脱した操作に関するログを記録し、警告を発する。	・AWSクラウドは、システムに対するアクセスログ等を取得し確認するための機能を提供しており、ログの取得・確認を行うことが可能。（詳細は、「6.1.4 (1) ログの取得・管理」参照。 ・AWS上に構築可能なログ管理サービスを利用し、アプリケーション経由で、誰が、どのデータにアクセスしたかのログを記録/保管することが可能。	・Amazon Relational Database Service (Amazon RDS) は、クラウド上でリレーショナルデータベースを簡単にセットアップ、運用、拡大/縮小できるウェブサービスです。業界標準のリレーショナルデータベース向けに、費用対効果に優れた拡張機能を備え、一般的なデータベース管理タスクを管理します。 ・MySQL、MariaDB、PostgreSQL、Oracle、Microsoft SQL Server などの使い慣れたデータベース製品のほか、MySQL と互換性のある新しい Amazon Aurora DB エンジンを使用できます (詳細は「Amazon RDS での Aurora（http://docs.aws.amazon.com/ja_jp/AmazonRDS/latest/UserGuide/CHAP_Aurora.html)」を参照)。 ・データベースパッケージのセキュリティに加え、AWS IAM を使用してユーザーとアクセス許可を定義すると、RDS データベースにアクセスできるユーザーを制御するのに役立ちます。また、Virtual Private Cloud に配置すると、データベースを保護することもできます。 詳細に関しては、http://docs.aws.amazon.com/ja_jp/AmazonRDS/latest/UserGuide/Welcome.html を参照してください。
7	7.2	7.2.4	(1)	(d)	情報システムセキュリティ責任者は、データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止するための対策を講ずること。	適合可能	・情報システムセキュリティ責任者は、データベースサーバ導入・運用にあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSの提供するDBサービス（Amazon RDS）を使う場合、データベース及びデータベースへアクセスする機器等の脆弱性を悪用したデータの不正な操作を防止するため、AWSの提供するAWS WAF （ウェブアプリケーションファイアウォール）の利用を考慮することが望ましい。 ・AWSの提供するAWS WAF （ウェブアプリケーションファイアウォール）にて、SQL インジェクションまたはクロスサイトスクリプトのような攻撃を防ぐルールを登録可能であり、これらの機能を踏まえた構成を考慮する必要がある。	・AWSクラウドは、SQL インジェクションまたはクロスサイトスクリプトのような一般的な攻撃パターンをブロックする機能を持つAWS WAF （ウェブアプリケーションファイアウォール）機能を提供しており、これらを利用し、脆弱性を利用した不正な操作を防止することが可能。	・AWS WAF は、お客様のウェブアプリケーションを、アプリケーションの可用性、セキュリティの侵害、リソースの過剰な消費などに影響を与えかねない一般的なウェブの弱点から保護するウェブアプリケーションファイアウォールです。AWS WAF を使用すると、カスタマイズ可能なウェブセキュリティルールを指定することによって、どのトラフィックをウェブアプリケーションに許可またはブロックするかを制御できます。AWS WAF を、SQL インジェクションまたはクロスサイトスクリプトのような一般的な攻撃パターンをブロックするカスタムルールおよび、特定のアプリケーションのために設計されるルールを作成するために利用できます。新しいルールは数分以内にデプロイされ、トラフィックパターンの変化に素早く対応できるようにします。また、AWS WAF は、フル機能の API を含んでいます。この API により、ウェブセキュリティルールの作成、デプロイ、メンテナンスを自動化することができます。 詳細に関しては、https://aws.amazon.com/jp/waf/ を参照してください。

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
7	7.2	7.2.4	(1)	(e)	情報システムセキュリティ責任者は、データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止する必要がある場合は、適切に暗号化をすること。	適合可能	・情報システムセキュリティ責任者は、データベースサーバ導入・運用にあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSの提供するDBサービス（Amazon RDS）を使う場合、Amazon RDS DB インスタンスの暗号化オプションの利用を考慮することが望ましい。但し、暗号化オプションを有効にすることで、保管時の Amazon RDS インスタンスとスナップショットの暗号化は可能であるものの、パスワードカラムの暗号化など、データベース上のデータの暗号化については、個別に検討を行う必要がある。	・AWSクラウドは、Amazon RDS DB インスタンスの暗号化オプションを提供しており、DBインスタンスの暗号化が可能。	セキュリティ ・Amazon RDSでは、AWS Key Management Service(KMS)を介して管理するキーを使って、データベースを暗号化できるようになりました。Amazon RDS暗号化を使用して実行するデータベースインスタンスでは、基盤となるストレージに保管されるデータが、自動バックアップ、リードレプリカ、スナップショットとして暗号化されます。 ・Amazon RDSは、SQL ServerおよびOracleのTransparent Data Encryptionをサポートします。OracleのTransparent Data Encryptionは、AWS CloudHSMと統合されています。これにより、AWSクラウド内のシングルテナントのHardware Security Module(HSM)アプライアンスで安全に暗号化キーを生成、保管、管理できます。 ・Amazon RDSは、通信中のデータを保護するSSLの使用に対応しています。 詳細に関しては、https://aws.amazon.com/jp/rds/details/#security を参照してください。 ・Amazon RDS DB インスタンスの暗号化オプションを有効にすることで、保管時の Amazon RDS インスタンスとスナップショットを暗号化できます。保管時に暗号化されるデータには、DB インスタンス、自動バックアップ、リードレプリカ、スナップショットの基本的なストレージが含まれます。 ・Amazon RDS の暗号化されたインスタンスでは、Amazon RDS インスタンスをホストしているサーバーでデータを暗号化するために、業界標準の AES-256 暗号化アルゴリズムを使用します。データが暗号化されると、Amazon RDS はパフォーマンスの影響を最小限に抑えながら、データへのアクセスと復号の認証を透過的に処理します。暗号化を使用するために、データベースのクライアントアプリケーションを変更する必要はありません。 ・Amazon RDS の暗号化されたインスタンスは、基になるストレージへの不正アクセスからデータを保護することによって、データ保護の追加レイヤーを提供します。Amazon RDS の暗号化を使用して、クラウドにデプロイされるアプリケーションのデータ保護を強化することや、および保管時のデータ暗号化に関するコンプライアンスの要件を達成することができます。 ・Amazon RDS は、Transparent Data Encryption (TDE) による Oracle または SQL Server の DB インスタンスの暗号化もサポートします。 詳細に関しては、http://docs.aws.amazon.com/ja_jp/AmazonRDS/latest/UserGuide/Overview.Encryption.html を参照してください。
7	7.3	通信回線							
7	7.3	7.3.1	通信回線						
7	7.3	7.3.1	(1)	通信回線の導入時の対策					
7	7.3	7.3.1	(1)	(a)	情報システムセキュリティ責任者は、通信回線構築時に、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じた適切な回線種別を選択し、情報セキュリティインシデントによる影響を回避するために、通信回線に対して必要な対策を講ずること。	適合可能	・情報システムにて取り扱う情報の格付及び取扱制限に応じた適切な回線種別を選択することについては、AWSクラウド利用有無にかかわらず情報システムセキュリティ責任者が検討するべき事項である。 ・情報システムセキュリティ責任者は、通信回線導入にあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド利用時には、AWSクラウドの提供するネットワークのセキュリティの仕組み（VPC、IPSecVPN、Direct Connect、AWS APIのSSL利用、セキュリティグループ）の利用を検討することが望ましい。 ・求められる機密性、完全性、可用性に応じ、専用線あるいはインターネットVPNの回線種別と回線・機器の冗長構成を選択する必要がある。 ・求められるネットワーク帯域に応じた、回線種別を選択する必要がある。	・AWSクラウドは、以下の機能を提供しており、これらを利用し、通信に対するセキュリティ対策を講ずることが可能。 　-Amazon VPC(Virtual Private Cloud)…AWS アカウント専用の仮想ネットワークであり、他の仮想ネットワークから論理的に切り離されるネットワークを提供。 　-IPSec ハードウェアVPN接続…業界標準で暗号化されたAWSクラウド上のインスタンスに対する接続を提供。 　-AWS Direct Connect…ユーザの設備からAWSへの専用ネットワーク接続を提供。 　-すべてのAWS APIは、SSLで保護されたエンドポイント経由で利用可能。 　-セキュリティグループ…お客様の Amazon EC2 インスタンスにアクセスするためのプロトコル、ポート、およびソース IP アドレス範囲の制御する仕組みを提供。	・Amazon Virtual Private Cloud(Amazon VPC)では、アマゾン ウェブ サービス(AWS)クラウドの論理的に分離したセクションがプロビジョニングされ、ここからお客様が定義する仮想ネットワークでAWSリソースを起動できます。独自のIPアドレス範囲の選択、サブネットの作成、ルーティングテーブルとネットワークゲートウェイの設定など、仮想ネットワーク環境を完全にコントロールできます。 ・VPC 内のインスタンスへ、およびインスタンスからのすべてのトラフィックは、業界標準で暗号化された IPsec ハードウェア VPN 接続を通して、自社のデータセンターへルーティングすることができます。 詳細に関しては、https://aws.amazon.com/jp/vpc/ を参照してください。 ・AWS Direct Connectにより、お客様の設備からAWSへの専用ネットワーク接続を簡単に確立することができます。AWS Direct Connectを使用すると、AWSとデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。 詳細に関しては、https://aws.amazon.com/jp/directconnect/ を参照してください。 ネットワークの監視と保護 ・すべてのAWS APIは、サーバー認証を提供する、SSLで保護されたエンドポイント経由で利用可能です。 セキュリティグループ ・セキュリティグループを使用して、お客様の Amazon EC2 インスタンスにアクセスするためのプロトコル、ポート、およびソース IP アドレス範囲を制御できます。つまり、これはお客様のインスタンスのファイアウォールルールを定義するものです。 詳細に関しては「セキュリティプロセスの概要（2014年11月）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf セキュリティグループは、インスタンスの仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィックをコントロールします。VPC内でインスタンスを起動した場合、そのインスタンスは最大 5 つのセキュリティグループに割り当てることができます。セキュリティグループは、サブネットレベルでなくインスタンスレベルで動作します。このため、VPC 内のサブネット内のインスタンスごとに異なるセキュリティグループのセットに割り当てることができます。起動時に特定のグループを指定しないと、インスタンスは VPC のデフォルトのセキュリティグループに自動的に割り当てられます。 セキュリティグループごとに、インスタンスへのインバウンドトラフィックをコントロールするルールと、アウトバウンドトラフィックをコントロールする一連のルールを個別に追加します。 詳細に関しては、http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html を参照してください。

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
7	7.3	7.3.1	(1)	(b)	情報システムセキュリティ責任者は、通信回線において、サーバ装置及び端末のアクセス制御及び経路制御を行う機能を設けること。	適合可能	・情報システムセキュリティ責任者は通信回線導入にあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド利用時には、AWSクラウドの提供するネットワークレベルのアクセス制御及び経路制御の仕組み（VPC、IPSecVPN、Direct Connect、AWS APIのSSL利用、セキュリティグループ）の利用を検討することが望ましい。 ・AWSクラウドではネットワークACL、セキュリティグループによるVPCへのアクセスを制限することは可能であるが、通信回線に接続するためのネットワーク機器（ルータ、L3スイッチ、ファイアウォール等）においても必要に応じたアクセス制限を行う必要がある。 ・AWSクラウドと接続する利用者環境側にもアクセス制御可能なネットワーク機器（ルータ、L3スイッチ、ファイアウォール等）の設置要否を検討する必要がある。	・AWSクラウドは、以下の機能を提供しており、これらを利用し、通信におけるアクセス制御や経路制御が可能。 -Amazon VPC(Virtual Private Cloud)…AWS アカウント専用の仮想ネットワークであり、他の仮想ネットワークから論理的に切り離されるネットワークを提供。 -IPSec ハードウェアVPN接続…業界標準で暗号化されたAWSクラウド上のインスタンスに対する接続を提供。 -AWS Direct Connect…ユーザの設備からAWSへの専用ネットワーク接続を提供。 -すべてのAWS APIは、SSLで保護されたエンドポイント経由で利用可能。 -セキュリティグループ…お客様の Amazon EC2 インスタンスにアクセスするためのプロトコル、ポート、およびソース IP アドレス範囲の制御する仕組みを提供。	・Amazon Virtual Private Cloud(Amazon VPC)では、アマゾン ウェブ サービス(AWS)クラウドの論理的に分離したセクションがプロビジョニングされ、ここからお客様が定義する仮想ネットワークでAWSリソースを起動できます。独自のIPアドレス範囲の選択、サブネットの作成、ルーティングテーブルとネットワークゲートウェイの設定など、仮想ネットワーク環境を完全にコントロールできます。 ・VPC 内のインスタンスへ、およびインスタンスからのすべてのトラフィックは、業界標準で暗号化された IPsec ハードウェア VPN 接続を通して、自社のデータセンターへルーティングすることができます。 詳細に関しては、https://aws.amazon.com/jp/vpc/ を参照してください。 ・AWS Direct Connectにより、お客様の設備からAWSへの専用ネットワーク接続を簡単に確立することができます。AWS Direct Connectを使用すると、AWSとデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。 詳細に関しては、https://aws.amazon.com/jp/directconnect/ を参照してください。 ネットワークの監視と保護 ・すべてのAWS APIは、サーバー認証を提供する、SSLで保護されたエンドポイント経由で利用可能です。 セキュリティグループ ・セキュリティグループを使用して、お客様の Amazon EC2 インスタンスにアクセスするためのプロトコル、ポート、およびソース IP アドレス範囲を制御できます。つまり、これはお客様のインスタンスのファイアウォールルールを定義するものです。 詳細に関しては「セキュリティプロセスの概要（2014年11月）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf セキュリティグループは、インスタンスの仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィックをコントロールします。VPC内でインスタンスを起動した場合、そのインスタンスは最大 5 つのセキュリティグループに割り当てることができます。セキュリティグループは、サブネットレベルでなくインスタンスレベルで動作します。このため、VPC 内のサブネット内のインスタンスごとに異なるセキュリティグループのセットに割り当てることができます。起動時に特定のグループを指定しないと、インスタンスは VPC のデフォルトのセキュリティグループに自動的に割り当てられます。 セキュリティグループごとに、インスタンスへのインバウンドトラフィックをコントロールするルールと、アウトバウンドトラフィックをコントロールする一連のルールを個別に追加します。 詳細に関しては、http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html を参照してください。
7	7.3	7.3.1	(1)	(c)	情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講ずること。	適合可能	・情報システムセキュリティ責任者は通信回線導入にあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド利用時には、通信内容の秘匿性を確保するための措置として、AWS Direct Connectや、IPSec ハードウェアVPN接続の利用を検討することが望ましい。 ・Direct Connect利用時には、通信データの盗聴、改ざんのリスクがあることを踏まえ、必要に応じてIPSecによる暗号化を実施する必要がある。 IPSecハードウェアVPN接続の場合は、IPSecによる暗号化が行われるためこの限りではない。	・AWSクラウドは、以下の機能を提供しており、これらを利用し、通信内容の秘匿が可能。 -IPSec ハードウェアVPN接続…業界標準で暗号化されたAWSクラウド上のインスタンスに対する接続を提供。 -AWS Direct Connect…ユーザの設備からAWSへの専用ネットワーク接続を提供。	・Amazon Virtual Private Cloud(Amazon VPC)では、アマゾン ウェブ サービス(AWS)クラウドの論理的に分離したセクションがプロビジョニングされ、ここからお客様が定義する仮想ネットワークでAWSリソースを起動できます。独自のIPアドレス範囲の選択、サブネットの作成、ルーティングテーブルとネットワークゲートウェイの設定など、仮想ネットワーク環境を完全にコントロールできます。 ・VPC 内のインスタンスへ、およびインスタンスからのすべてのトラフィックは、業界標準で暗号化された IPsec ハードウェア VPN 接続を通して、自社のデータセンターへルーティングすることができます。 詳細に関しては、https://aws.amazon.com/jp/vpc/ を参照してください。 ・AWS Direct Connectにより、お客様の設備からAWSへの専用ネットワーク接続を簡単に確立することができます。AWS Direct Connectを使用すると、AWSとデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。 詳細に関しては、https://aws.amazon.com/jp/directconnect/ を参照してください。
7	7.3	7.3.1	(1)	(d)	情報システムセキュリティ責任者は、職員等が通信回線へ情報システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずること。機関等内通信回線へ機関等支給以外の端末を接続する際も同様とする。	適合可能	・情報システムセキュリティ責任者は通信回線導入にあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド利用時には、従来のシステムと同様に、定められた手続き、手順に従い必要な承認を得た上で接続する必要がある。 ・AWSクラウドでインターネットとの接続を許可している場合は、許可された情報システムのみを接続し、許可されない利用を抑止するためのProxyサーバやファイアウォールでの接続遮断等の技術的対策を併せて実施する必要がある。VPCでインターネットゲートウェイを設定しない場合は、VPC環境から直接インターネットへ通信させないことも可能。 ・ AWSクラウド側で端末を識別する対策も選択肢に含めて検討する必要がある。	・AWSクラウドは、以下の機能を提供しており、これらを利用し、通信内回線への接続を制御可能。 -Amazon VPC(Virtual Private Cloud)…AWS アカウント専用の仮想ネットワークであり、他の仮想ネットワークから論理的に切り離されるネットワークを提供。 -IPSec ハードウェアVPN接続…業界標準で暗号化されたAWSクラウド上のインスタンスに対する接続を提供。 -AWS Direct Connect…ユーザの設備からAWSへの専用ネットワーク接続を提供。 -すべてのAWS APIは、SSLで保護されたエンドポイント経由で利用可能。 -セキュリティグループ…お客様の Amazon EC2 インスタンスにアクセスするためのプロトコル、ポート、およびソース IP アドレス範囲の制御する仕組みを提供。	・Amazon Virtual Private Cloud(Amazon VPC)では、アマゾン ウェブ サービス(AWS)クラウドの論理的に分離したセクションがプロビジョニングされ、ここからお客様が定義する仮想ネットワークでAWSリソースを起動できます。独自のIPアドレス範囲の選択、サブネットの作成、ルーティングテーブルとネットワークゲートウェイの設定など、仮想ネットワーク環境を完全にコントロールできます。 ・VPC 内のインスタンスへ、およびインスタンスからのすべてのトラフィックは、業界標準で暗号化された IPsec ハードウェア VPN 接続を通して、自社のデータセンターへルーティングすることができます。 詳細に関しては、https://aws.amazon.com/jp/vpc/ を参照してください。 ・AWS Direct Connectにより、お客様の設備からAWSへの専用ネットワーク接続を簡単に確立することができます。AWS Direct Connectを使用すると、AWSとデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。 詳細に関しては、https://aws.amazon.com/jp/directconnect/ を参照してください。 ネットワークの監視と保護 ・すべてのAWS APIは、サーバー認証を提供する、SSLで保護されたエンドポイント経由で利用可能です。 セキュリティグループ ・セキュリティグループを使用して、お客様の Amazon EC2 インスタンスにアクセスするためのプロトコル、ポート、およびソース IP アドレス範囲を制御できます。つまり、これはお客様のインスタンスのファイアウォールルールを定義するものです。 詳細に関しては「セキュリティプロセスの概要（2014年11月）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf セキュリティグループは、インスタンスの仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィックをコントロールします。VPC内でインスタンスを起動した場合、そのインスタンスは最大 5 つのセキュリティグループに割り当てることができます。セキュリティグループは、サブネットレベルでなくインスタンスレベルで動作します。このため、VPC 内のサブネット内のインスタンスごとに異なるセキュリティグループのセットに割り当てることができます。起動時に特定のグループを指定しないと、インスタンスは VPC のデフォルトのセキュリティグループに自動的に割り当てられます。 セキュリティグループごとに、インスタンスへのインバウンドトラフィックをコントロールするルールと、アウトバウンドトラフィックをコントロールする一連のルールを個別に追加します。 詳細に関しては、http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html を参照してください。

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
7	7.3	7.3.1	(1)	(e)	情報システムセキュリティ責任者は、通信回線装置を要管理対策区域に設置すること。ただし、要管理対策区域への設置が困難な場合は、物理的な保護措置を講ずるなどして、第三者による破壊や不正な操作等が行われないようにすること。	適合可能	・AWSが取得しているISO27001等の認証でAWSクラウドデータセンター自体の物理セキュリティや、データセンター内の通信回線装置等の物理コンポーネント自体の物理セキュリティ対策を確認の上、ユーザでAWSクラウドを利用して導入・運用する情報システムのセキュリティ対策を検討する。	・AWSは、ISO27001等に準拠して、サーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威からの保護を行っており、利用者は、これらの認証を取得していることを確認可能である。なお、AWSは、第三者による審査・監査等により、この基準への準拠について認証を取得済みである。 ・AWS のデータセンターでは、物理的および環境のセキュリティとして以下のような対策を実施している。これらの対策により、サーバ装置の盗難、不正な持ち出し、サーバ装置の不正な操作等を防止することが可能。 -ビデオ監視カメラ、侵入検出システム -データセンターのフロアへのアクセス時の2 要素認証 -身分証明書の提示、署名、権限者の付き添い -データセンターへのすべての物理的アクセスを記録、監査 -特権を必要とする作業完了後アクセス権を速やかに取消し -AWS専有インベントリ管理ツールにて、資産の追跡および監視を行い、在庫の監査を定期的に実施。	データセンター セキュリティ 資産管理 ISO 27001基準に合わせて、AWSの担当者がAWS専有インベントリ管理ツールを使用して、AWSハードウェアの資産に所有者を割り当て、追跡および監視を行っています。AWSの調達およびサプライチェーンチームは、すべてのAWSサプライヤとの関係を維持しています。 詳細については、ISO 27001基準の付録A、ドメイン7.1を参照してください。AWSは、ISO 27001認定基準への対応を確認する独立監査人から、検証および認定を受けています。 詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf 物理的および環境のセキュリティ Amazon のデータセンターは最新式で、革新的で建築的かつ工学的アプローチを採用しています。Amazon は大規模データセンターの設計、構築、運用において、長年の経験を有しています。この経験は、AWS プラットフォームとインフラストラクチャに活かされています。AWS のデータセンターは、外部からはそれとはわからないようになっています。ビデオ監視カメラ、最新鋭の侵入検出システム、その他エレクトロニクスを使った手段を用いて、専門のセキュリティスタッフが、建物の入口とその周辺両方において、物理的アクセスを厳密に管理しています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行います。 AWS は、そのような権限に対して正規のビジネスニーズがある従業員や業者に対してのみデータセンターへのアクセスや情報を提供しています。従業員がこれらの特権を必要とする作業を完了したら、たとえかれらが引き続き Amazonまたは Amazon Web Services の従業員であったとしても、そのアクセス権は速やかに取り消されます。AWS 従業員によるデータセンターへのすべての物理的アクセスは記録され、定期的に監査されます。 詳細に関しては「セキュリティプロセスの概要（2014年11月）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf
7	7.3	7.3.1	(1)	(f)	情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムが接続される通信回線について、当該通信回線の継続的な運用を可能とするための措置を講ずること。	対象外	・要安定情報を取り扱う情報システムが接続される通信回線について、当該通信回線の継続的な運用を可能とするための措置を講ずることについては、クラウドサービス利用有無にかかわらず情報システムセキュリティ責任者が検討するべき事項である。	・当該内容については、本リファレンスの説明の対象外。	−
7	7.3	7.3.1	(1)	(g)	情報システムセキュリティ責任者は、機関等内通信回線にインターネット回線、公衆通信回線等の機関等外通信回線を接続する場合には、機関等内通信回線及び当該機関等内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずること。	対象外	・機関等内通信回線にインターネット回線、公衆通信回線等の機関等外通信回線を接続する場合には、機関等内通信回線及び当該機関等内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずることについては、クラウドサービス利用有無にかかわらず情報システムセキュリティ責任者が検討するべき事項である。	・当該内容については、本リファレンスの説明の対象外。	−
7	7.3	7.3.1	(1)	(h)	情報システムセキュリティ責任者は、機関等内通信回線と機関等外通信回線との間で送受信される通信内容を監視するための措置を講ずること。	対象外	・機関等内通信回線と機関等外通信回線との間で送受信される通信内容を監視するための措置を講ずることについては、クラウドサービス利用有無にかかわらず情報システムセキュリティ責任者が検討するべき事項である。	・当該内容については、本リファレンスの説明の対象外。	−
7	7.3	7.3.1	(1)	(i)	情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアを定め、ソフトウェアを変更する際の許可申請手順を整備すること。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。	適合可能	・AWSで取得しているSOC 1 Type II レポートでソフトウェアの変更管理に関するセキュリティ対策を確認の上、ユーザでAWSクラウドを利用して導入・運用する情報システムのセキュリティ対策をを選択する。 [留意事項] ・AWSクラウドを利用する場合、システム構成やソフトウェアの状態を定期的に確認する情報の記録については、AWSクラウドの提供する機能(AWS Config)を利用することが望ましい。	・利用者は、AWSが変更管理に関し、既存の IT リソースに対する変更がある場合、当該内容が記録され、認証され、試験され、承認され、文書化されることについて合理的な保証を提供し統制目標として特定されていることについて、SOC 1 Type II レポートにて、独立監査人によって保証されていることを確認可能である。 ・AWSクラウドは、AWS Configサービスにて、AWS リソースインベントリ、設定履歴、および設定変更通知といった機能を提供する。また、既存のAWS リソースと削除された AWS リソースとの検出、ルールに対する全体的なコンプライアンスの判定、および任意の時点でのリソース設定の詳細な調査が可能。	・アマゾン ウェブ サービスは現在、Service Organization Controls 1 (SOC 1)、Type II レポートを発行しています。 レポートには AWS SOC 1 の統制目標が記載されており、このレポート自体に、各統制目標と独立監査人による各統制のテスト手順の結果をサポートする統制活動が特定されています。 変更管理 ・統制は、既存の IT リソースに対する変更 (緊急/特殊な設定) が記録され、認証され、試験され、承認されて文書化されることについて、合理的な保証を提供するものです。 詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf ソフトウェア AWS は、変更の管理にシステム的なアプローチを採用しています。そのためお客様に影響を与えるサービスの変更は、徹底的に検証、テスト、承認され、充分な情報が提供されます。AWS の変更管理プロセスは、意図しないサービス障害を防ぎ、お客様に対するサービスの完全性を維持することを目的としています。実稼働環境にデプロイされる変更には、以下の対応が行われます: • 検証: 変更の技術的側面について専門家による検証が必要です。 • テスト: 適用されている変更は、予想どおりに動作し、パフォーマンスに悪影響を与えないことを確認するためにテストされます。 • 承認: すべての変更は、ビジネスへの影響を適切に監視し、それらの影響についての情報を提供するために、承認される必要があります。 詳細に関しては「セキュリティプロセスの概要（2014年11月）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf AWS Config は完全マネージド型のサービスで、セキュリティとガバナンスのため、AWS リソースインベントリ、設定履歴、および設定変更通知といった機能が用意されています。Config Rules を使用して、AWS Config によって記録された AWS リソース設定を自動的にチェックするルールを作成できます。 AWS Config を使用することで、既存の AWS リソースと削除された AWS リソースとの検出、ルールに対する全体的なコンプライアンスの判定、および任意の時点でのリソース設定の詳細な調査が可能になります。これらの機能は、コンプライアンス監査、セキュリティ分析、リソース変更の追跡、トラブルシューティングを可能にします。 詳細に関しては、https://aws.amazon.com/jp/config/ を参照してください。

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
7	7.3	7.3.1	(1)	(j)	情報システムセキュリティ責任者は、保守又は診断のために、遠隔地から通信回線装置に対して行われるリモートアクセスに係る情報セキュリティを確保すること。	適合可能	・情報システムセキュリティ責任者は通信回線導入にあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド利用時には、通信内容の秘匿性を確保するための措置として、AWS Direct Connectや、IPSec ハードウェアVPN接続の利用を検討することが望ましい。 ・Direct Connect利用時には、通信データの盗聴、改ざんのリスクがあることを踏まえ、必要に応じてIPSecやSSLでの暗号化を実施する必要がある。IPSecハードウェアVPN接続の場合は、IPSecによる暗号化が行われるためこの限りではない。	・AWSクラウドは、以下の機能を提供する。これにより、通信の暗号化等、リモートアクセスに係る情報セキュリティ対策を実施することが可能。 -IPSec ハードウェアVPN接続…業界標準で暗号化されたAWSクラウド上のインスタンスに対する接続を提供。 -AWS Direct Connect…ユーザの設備からAWSへの専用ネットワーク接続を提供。	・Amazon Virtual Private Cloud(Amazon VPC)では、アマゾン ウェブ サービス(AWS)クラウドの論理的に分離したセクションがプロビジョニングされ、ここからお客様が定義する仮想ネットワークでAWSリソースを起動できます。独自のIPアドレス範囲の選択、サブネットの作成、ルーティングテーブルとネットワークゲートウェイの設定など、仮想ネットワーク環境を完全にコントロールできます。 ・VPC 内のインスタンスへ、およびインスタンスからのすべてのトラフィックは、業界標準で暗号化された IPsec ハードウェア VPN 接続を通して、自社のデータセンターへルーティングすることができます。 詳細に関しては、https://aws.amazon.com/jp/vpc/ を参照してください。 ・AWS Direct Connectにより、お客様の設備からAWSへの専用ネットワーク接続を簡単に確立することができます。AWS Direct Connectを使用すると、AWSとデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。 詳細に関しては、https://aws.amazon.com/jp/directconnect/ を参照してください。
7	7.3	7.3.1	(1)	(k)	情報システムセキュリティ責任者は、電気通信事業者の通信回線サービスを利用する場合には、当該通信回線サービスの情報セキュリティ水準及びサービスレベルを確保するための措置について、情報システムの構築を委託する事業者と契約時に取り決めておくこと。	対象外	・通信回線サービスの情報セキュリティ水準及びサービスレベルを確保するための措置について、情報システムの構築を委託する事業者と契約時に取り決めておくことについては、クラウドサービス利用有無にかかわらず情報システムセキュリティ責任者が検討するべき事項である。	・通信回線サービスの情報セキュリティ水準及びサービスレベルを確保するための措置について、情報システムの構築を委託する事業者と契約時に取り決めておくことについては、本リファレンスの説明の対象外。	–
7	7.3	7.3.1	(2)	通信回線の運用時の対策					
7	7.3	7.3.1	(2)	(a)	情報システムセキュリティ責任者は、情報セキュリティインシデントによる影響を防止するために、通信回線装置の運用時に必要な措置を講ずること。	適合可能	・AWSクラウドにおける情報セキュリティインシデントによる影響を防止する対策は、AWSクラウド自身で管理する。これを踏まえて、情報システムセキュリティ責任者は、AWSクラウドを利用して情報システムを導入・運用するか否かについて判断する必要がある。また、AWSクラウドを利用して導入・運用する情報システムのセキュリティ対策を検討し対策を講ずることについては、ユーザ責任で実施する必要がある。 [留意事項] ・情報セキュリティ責任者が導入した通信回線装置（クラウドサービス事業者が導入する装置以外の装置）の運用において、情報セキュリティインシデントによる影響を防止するために、通信回線装置の運用時に必要な措置を講ずることは、クラウドサービス利用有無にかかわらず情報システムセキュリティ責任者が検討するべき事項である。	・AWSクラウドは、インシデントへの対応として、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く。作業員スタッフが、24 時間 365 日体制でインシデントを検出し、影響と解決方法を管理する。 ・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備えている。（以下に例示） - 分散型サービス妨害（DDoS）攻撃対策…専属的なDDoS 緩和技術を使用 - 中間者（MITM）攻撃対策…すべての AWS API に、サーバー認証を提供 -IP スプーフィング対策…なりすましたネットワークトラフィックの送信不許可 - ポートスキャン対策…不正なポートスキャンが AWS によって検出された場合、停止およびブロック - 第三者によるパケットスニッフィング対策…仮想インスタンスが、異なる仮想インスタンス向けのトラフィックを受信または "傍受"することを禁止	セキュリティインシデント処理 Amazon のインシデント管理チームは、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 日体制でインシデントを検出し、影響と解決方法を管理します。AWS の事故対応プログラム、計画、および手続きは、ISO 27001 基準に合わせて作成されています。AWS SOC 1 Type II レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。 詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf ネットワークの監視と保護 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備えており、さらに堅牢な保護を実装することができます。以下にいくつかの例を示します: • 分散型サービス妨害（DDoS）攻撃。専属的なDDoS 緩和技術が使用されています。さらに、AWS ネットワークは、複数のプロバイダによるマルチホーム構成になっていて、インターネットアクセスの多様化を実現しています。 • 中間者（MITM）攻撃。すべての AWS API は、サーバー認証を提供する、SSL で保護されたエンドポイント経由で利用可能ですAWS とのやり取りにはすべてSSL を使用することをお勧めします。 • IP スプーフィング。Amazon EC2 インスタンスは、なりすましたネットワークトラフィックを送信できません。AWS によって管理される、ホストベースのファイアウォールインフラストラクチャでは、インスタンスは、ソース IP またはMAC アドレスがインスタンス自身のものでないトラフィックを送信できません。 • ポートスキャン。不正なポートスキャンが AWS によって検出された場合、停止およびブロックされます。Amazon EC2 インスタンスのインバウンドポートはすべてデフォルトで閉じられており、お客様によってのみ開かれるため、Amazon EC2 インスタンスのポートスキャンは、一般的には効果がありません。セキュリティグループを厳格に管理することによって、ポートスキャンの脅威をより軽減できます。 • 第三者によるパケットスニッフィング。無差別モード（プロミスキャスモード）で実行中の仮想インスタンスが、異なる仮想インスタンス向けのトラフィックを受信または "傍受" することはできません。インターフェイスをプロミスキャスモードにすることはできますが、ハイパーバイザーは宛先に指定されていないインターフェイスにトラフィックを伝送しません。物理的に同一のホスト上に配置された、同一の顧客によって保有される 2 つの仮想インスタンスであっても、互いのトラフィックを傍受することはできません。 詳細に関しては「セキュリティプロセスの概要（2014年11月）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf
7	7.3	7.3.1	(2)	(b)	情報システムセキュリティ責任者は、経路制御及びアクセス制御を適切に運用し、通信回線や通信要件の変更の際及び定期的に、経路制御及びアクセス制御の設定の見直しを行うこと。	対象外	・通信回線や通信要件の変更の際及び定期的に、経路制御及びアクセス制御の設定の見直しを行うこととについては、クラウドサービス利用有無にかかわらず情報システムセキュリティ責任者が検討するべき事項である。	・通信回線や通信要件の変更の際及び定期的な経路制御及びアクセス制御の設定の見直しについては、本リファレンスの説明の対象外。	–
7	7.3	7.3.1	(2)	(c)	情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアの状態を定期的に調査し、許可されていないソフトウェアがインストールされているなど、不適切な状態にある通信回線装置を認識した場合には、改善を図ること。	対象外	・情報セキュリティ責任者が導入した通信回線装置（クラウドサービス事業者が導入する装置以外の装置）に関し、許可されていないソフトウェアがインストールされているなど、不適切な状態にある通信回線装置を認識した場合の改善対応については、クラウドサービス利用有無にかかわらず情報システムセキュリティ責任者が検討するべき事項である。	・AWSクラウドで導入する装置以外の通信回線装置の運用については、AWSクラウドの対象外。	–
7	7.3	7.3.1	(2)	(d)	情報システムセキュリティ責任者は、情報システムの情報セキュリティの確保が困難な事由が発生した場合には、当該情報システムが他の情報システムと共有している通信回線について、共有先の他の情報システムを保護するため、当該通信回線とは別に独立した閉鎖的な通信回線に構成を変更すること。	対象外	・AWSクラウドのAmazon VPC(Virtual Private Cloud)は、AWS アカウント専用の仮想ネットワークであり、他の仮想ネットワークから論理的に切り離されるネットワークとして提供されるが、 情報システムの情報セキュリティの確保が困難な事由が発生した場合に独立した閉鎖的な通信回線に構成を変更することについては、AWSクラウドにおいては対応できないため、情報システムセキュリティ責任者が検討するべき事項である。	・AWSクラウドでは、仮想ネットワークを提供しているが、本リファレンスの説明の対象外。	–
7	7.3	7.3.1	(3)	通信回線の運用終了時の対策					

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
7	7.3	7.3.1	(3)	(a)	情報システムセキュリティ責任者は、通信回線装置の運用を終了する場合には、当該通信回線を構成する通信回線装置が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた情報が漏えいすることを防止するため、当該通信回線装置の電磁的記録媒体に記録されている全ての情報を抹消するなど適切な措置を講ずること。	適合可能	・AWSが取得しているISO27001の認証でAWSクラウドデータセンター内のサーバやストレージ等のハードウェアデバイスの廃棄やデータ消去に関するセキュリティ対策を確認の上、ユーザでAWSクラウドを利用して導入・運用する情報システムのセキュリティ対策をを選択する。 [留意事項] ・AWSクラウド利用時には、AWSクラウド上の物理ディスク上からゼロWrite等の処理により物理的にデータの抹消ができない場合、別途データ暗号化を行っておき、システム運用終了時に暗号化のための鍵データを削除するといったデータ抹消相当の対応を考慮する必要がある。	・AWSは、ISO27001に準拠して、ストレージデバイスが製品寿命に達した場合、以下いずれかに記載されている技術を用いて廃棄プロセスの一環としてデータを破棄しており、利用者は、これらの認証を取得していることを確認可能である。 - DoD5220.22-M - NIST800-88 また、ハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁又は物理的に破壊する。	AWSの処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWSは、DoD 5220.22-M（「National Industrial Security Program OperatingManual（国立産業セキュリティプログラム作業マニュアル）」）またはNIST 800-88（「Guidelines for Media Sanitization（メディア衛生のためのガイドライン）」）に詳細が記載されている技術を用いて、廃棄プロセスの一環としてデータを破棄します。廃棄された磁気ストレージデバイスはすべて業界標準の方法に従って消磁され、物理的に破壊されます。 詳細に関しては「セキュリティプロセスの概要（2014年11月）」をご参照下さい。 https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf ISO27001基準に合わせて、AWSの処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWSはDoD5220.22-MまたはNIST800-88に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。 詳細については、ISO27001規格の附属書A、ドメイン9.2を参照してください。AWSは、ISO27001認定基準への対応を確認する独立監査人から、検証および認定を受けています。 詳細に関しては「リスクおよびコンプライアンス（2015年8月）」をご参照下さい。 http://d0.awsstatic.com/whitepapers/International/jp/AWS_Risk_Compliance_Whitepaper_Aug_2015.pdf データの永続性 データは、ボリュームを明示的に削除するまでボリュームに保持されます。削除した EBS ボリュームが使用していた物理的なブロックストレージは、別のアカウントに割り当てられる前に、ゼロで上書きされます。機密データを扱っている場合は、手動によるデータの暗号化や、Amazon EBS 暗号化 で保護されているボリュームへのデータの格納を検討してください。詳細については、「Amazon EBS Encryption」を参照してください。 デフォルトでは、インスタンスの起動時に作成およびアタッチされた EBS ボリュームは、インスタンスの終了時に削除されます。この動作を変更するには、インスタンスの起動時にフラグ DeleteOnTermination の値を false に変更します。値を変更すると、インスタンスが終了してもボリュームが保持されるので、そのボリュームを別のインスタンスにアタッチできます。 詳細に関しては、http://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSVolumes.html を参照してください。 13. AWS Import/Export 13.14 アプライアンスの外的状況にかかわらず、また、サービス利用者が、アプライアンスが損傷しているまたは機能していない可能性があると考える場合であっても、サービス利用者はアマゾンに対して、全てのアプライアンスを返却するものとする。アプライアンスは廃電気・電子機器ではなく、また、サービス利用者はアプライアンスの最終ユーザーとはならないが、疑義を避けるために付言すると、サービス利用者は、アプライアンスが廃電気・電子機器として（未分類市町村廃棄物とされる場合を含む）、またはその他の廃棄物収集過程において処分されるものではないこと、本契約の条項に従ったサービス利用者による使用されたアプライアンスのアマゾンへの返却が、アプライアンスの耐用年数の延長およびアプライアンスが耐用年数に達したときのアマゾンによるその責任ある取扱およびリサイクルに貢献すること、また、その他の電子・電気機器と同様、かかる機器における有害物質の存在の結果、アプライアンスの処分または不適切な取扱が、環境および人の健康に悪影響を与える可能性があることを了解するものとする。疑義を避けるために述べると、本項の条件はアプライアンスに含まれる内蔵バッテリーにも適用される。サービス利用者は、アプライアンスの内蔵バッテリーにアクセスしまたはこれを移動もしくは移転してはならない。アプライアンスは、かかる要件を反映するため、および一定の管轄地域における廃棄物関連の規制要件に従って、クロストアウト・ホイール・ビンのシンボルマークが付されている。 詳細に関しては、https://aws.amazon.com/jp/service-terms/ を参照してください。
7	7.3	7.3.1	(4)	リモートアクセス環境導入時の対策					
7	7.3	7.3.1	(4)	(a)	情報システムセキュリティ責任者は、職員等の業務遂行を目的としたリモートアクセス環境を、機関等外通信回線を経由して機関等の情報システムへリモートアクセスする形態により構築する場合は、VPN 回線を整備するなどして、通信経路及びアクセス先の情報システムのセキュリティを確保すること。	適合可能	・情報システムセキュリティ責任者は、システム導入・運用にあたり、AWSクラウドを利用する場合も、AWSクラウド利用の無い従来の情報システムと同様の検討（設計、構築、運用等）を行う必要がある。 [留意事項] ・AWSクラウド利用時には、通信内容の秘匿性を確保するための措置として、AWS Direct Connectや、IPSec ハードウェアVPN接続の利用を検討することが望ましい。 ・リモートアクセスにおいて使用する通信経路はIPSec あるいはSSLによる暗号化によりデータ伝送中に機密性、完全性を確保する必要がある。 ・職員等がリモートアクセスにより利用可能となる情報システムは、業務上の必要性のみならず、情報システムの取り扱う情報の格付及び取扱制限に従い、必要最低限の許可に制限する必要がある。	・AWSクラウドは、以下の機能を提供しており、これらを利用し、通信経路及びアクセス先の情報システムのセキュリティを確保可能。 -IPSec ハードウェアVPN接続…業界標準で暗号化されたAWSクラウド上のインスタンスに対する接続を提供。 -AWS Direct Connect…ユーザの設備からAWSへの専用ネットワーク接続を提供。	・Amazon Virtual Private Cloud(Amazon VPC)では、アマゾン ウェブ サービス(AWS)クラウドの論理的に分離したセクションがプロビジョニングされ、ここからお客様が定義する仮想ネットワークでAWSリソースを起動できます。独自のIPアドレス範囲の選択、サブネットの作成、ルーティングテーブルとネットワークゲートウェイの設定など、仮想ネットワーク環境を完全にコントロールできます。 ・VPC 内のインスタンスへ、およびインスタンスからのすべてのトラフィックは、業界標準で暗号化された IPsec ハードウェア VPN 接続を通して、自社のデータセンターへルーティングすることができます。 詳細に関しては、https://aws.amazon.com/jp/vpc/ を参照してください。 ・AWS Direct Connectにより、お客様の設備からAWSへの専用ネットワーク接続を簡単に確立することができます。AWS Direct Connectを使用すると、AWSとデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。 詳細に関しては、https://aws.amazon.com/jp/directconnect/ を参照してください。
7	7.3	7.3.1	(5)	無線LAN 環境導入時の対策					
7	7.3	7.3.1	(5)	(a)	情報システムセキュリティ責任者は、無線 LAN 技術を利用して機関等内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、通信内容の秘匿性を確保するために通信路の暗号化を行った上で、その他の情報セキュリティ確保のために必要な措置を講ずること。	対象外			–
7	7.3	7.3.2	IPv6 通信回線						
7	7.3	7.3.2	(1)	IPv6 通信を行う情報システムに係る対策					
7	7.3	7.3.2	(1)	(a)	情報システムセキュリティ責任者は、IPv6 技術を利用する通信を行う情報システムを構築する場合は、製品として調達する機器等について、IPv6 Ready Logo Program に基づく Phase-2 準拠製品を、可能な場合には選択すること。	対象外			–
7	7.3	7.3.2	(1)	(b)	情報システムセキュリティ責任者は、IPv6 通信の特性等を踏まえ、IPv6 通信を想定して構築する情報システムにおいて、以下の事項を含む脅威又は脆弱性に対する検討を行い、必要な措置を講ずること。	対象外			–
7	7.3	7.3.2	(1)	(b)	(ア) グローバル IP アドレスによる直接の到達性における脅威	対象外			–
7	7.3	7.3.2	(1)	(b)	(イ) IPv6 通信環境の設定不備等に起因する不正アクセスの脅威	対象外			–
7	7.3	7.3.2	(1)	(b)	(ウ) IPv4 通信と IPv6 通信を情報システムにおいて共存させる際の処理考慮漏れに起因する脆弱性の発生	対象外			–
7	7.3	7.3.2	(1)	(b)	(エ) アプリケーションにおける IPv6 アドレスの取扱い考慮漏れに起因する脆弱性の発生	対象外			–
7	7.3	7.3.2	(2)	意図しないIPv6 通信の抑止・監視					

部	章	節	項	項目	遵守事項	AWSクラウドにて提供するサービス/機能による統一基準への適合性	AWSクラウド利用におけるユーザーの対応指針	AWSクラウドで実現可能なこと	AWSクラウドの情報（2018年12月現在）
7	7.3	7.3.2	(2)	(a)	情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置を、IPv6 通信を想定していない通信回線に接続する場合には、自動トンネリング機能で想定外の IPv6 通信パケットが到達する脅威等、当該通信回線から受ける不正なIPv6 通信による情報セキュリティ上の脅威を防止するため、IPv6 通信を抑止するなどの措置を講ずること。	対象外			–