

AWS における経済安全保障推進法に関する考慮事項 (日本語)

May 17, 2024



Notices

お客様は、本文書に記載されている情報を独自に評価する責任があります。本文書は (a)情報提供のみを目的とし、(b)現在の AWS 製品の提供と実践を表しており、これらは予告なしに変更されることがあり、(c)AWS およびその関連会社、サプライヤー、ライセンサーからのいかなる約束または保証も生じません。AWS の製品またはサービスは、明示または黙示を問わず、いかなる種類の保証、表明、または条件もなく、「現状のまま」提供されます。AWS のお客様に対する責任および義務は、AWS の契約によって管理されており、本文書は AWS とお客様との間の契約の一部ではなく、またそれを変更するものでもありません。

本文書は、発行日時点の情報に基づき、記載しております。最新の状況は適宜ご確認ください。

© 2024 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Contents

1	対象読者	v
2	経済安全保障推進法の概要	1
3	クラウドサービスの利用における留意事項	2
4	Amazon Web Services のシステムの概要	4
5	AWS における経済安全保障推進法への対応	7
1.	お客様が実施すべき事項	7
2.	「導入等計画書」 「4. 構成設備に関する事項」	7
3.	「導入等計画書」 「5. 特定重要設備の導入にあたって特定社会基盤事業者が講ずる 特定妨害行為を防止するための措置に係る事項」に関する考慮事項（共通項目）	7
4.	その他規制業種毎の個別要求項目	19
	Document Revisions	20

1 対象読者

本文書の対象読者は、「「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律に基づく特定社会基盤事業者の指定等に関する内閣府令の一部を改正する内閣府令」にもとづき、クラウドサービスである Amazon Web Services (AWS) を、自らが提供もしくは供給する特定重要設備の構成設備として利用するお客様、もしくはその構成を評価する調達府省庁等の担当者様等において AWS の理解を深めることを目的とした組織の関係者にも参考となるものです。

本文書で取り上げている AWS サービスの構成方法の詳細については、担当の AWS ソリューションアーキテクトにお問い合わせください。

今後の関連法令の施行および関連ガイドラインなどの発行により、変更が予想されることをご留意ください。

2 経済安全保障推進法の概要

内閣府 HP によれば、経済安全保障推進法の趣旨は次を目的としたものとなります。

“この法律は、国際情勢の複雑化、社会経済構造の変化等に伴い、安全保障を確保するためには、経済活動に関して行われる国家及び国民の安全を害する行為を未然に防止する重要性が増大していることに鑑み、安全保障の確保に関する経済施策を総合的かつ効果的に推進するため、経済施策を一体的に講ずることによる安全保障の確保の推進に関する基本方針を策定するとともに、安全保障の確保に関する経済施策として、所要の制度を創設するものです。

具体的には、法制上の手当てが必要な喫緊の課題に対応するため、(1)重要物資の安定的な供給の確保、(2)基幹インフラ役務の安定的な提供の確保、(3)先端的な重要技術の開発支援、(4)特許出願の非公開に関する 4 つの制度を創設するものです。”

https://www.cao.go.jp/keizai_anzen_hosho/

同法では、「基幹インフラ役務の安定的な提供の確保」を目的として、“基幹インフラの重要設備が我が国の外部から行われる役務の安定的な提供を妨害する行為の手段として使用されることを防止するため、重要設備の導入・維持管理等の委託の事前審査、勧告・命令等を措置”（内閣府「経済安全保障推進法の概要」）を位置づけており、AWS のお客様が同法に該当する対象事業者である場合や、対象事業を目的としてサービスを提供する供給者である場合に適切な管理を行うことを求めています。

3 クラウドサービスの利用における留意事項

・対象となる事業者

経済安全保障推進法では、特定社会基盤事業として、“法第 50 条第 1 項各号に掲げる事業の中から、特定社会基盤役務（「①国民生活又は経済活動が依存している役務であって、その利用を欠くことにより、広範囲又は大規模な社会混乱を生ずるなどの経済・社会秩序の平穩を損なう事態が生じ得るもの」又は②「国民の生存に不可欠な役務であって、その代替が困難であるもの」）の提供を行うもの”を政令で定め、指定しています。

対象の業種及びシステムは各省庁のホームページなどをご参照ください。

指定された事業者は対象となる特定重要設備（後述）に関して、「導入等計画書」により省令に定められた監督官庁に届け出を行うことが求められます。これは、特定重要設備がサービスの停止やサイバー攻撃などのリスクの可能性を低減させるための措置を有効に実施しているかを事業者自らがリスク評価し、リスク管理措置の妥当性を届出内容により判断することを目的としています。

・特定重要設備と構成設備

特定重要設備：お客様の責任

特定社会基盤事業を営むうえで対象となるシステムを「特定重要設備」とし、例えば電気事業における一般送配電事業を営むための需給制御システムや系統制御システムがこれにあたります。こうした対象となる「特定重要設備」は各省庁からの省令で定められます。このような「特定重要設備」に関しては「特定重要設備の供給者」として、「特定重要設備」自体の開発や運用、保守に携わる利害関係者が存在し、お客様は適切なコミュニケーションを行う責任があります。

構成設備：AWS の責任

また、このような「特定重要設備」は様々なサービスの構成要素からなります。AWS をご利用のお客様はこのようなシステムの構成要素の一部としてクラウドをご利用いただくことになります。経済安全保障推進法では、こうしたサービスの構成要素を「構成設備」として定義し、法の定義において求められる要件を定めています。

なお、特定重要設備は複数の構成設備から構成される場合があります。お客様は特定重要設備がどのような構成設備を含むのかを適切に評価する必要があります。

・経済安全保障推進法と ISMAP の関係

政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））は、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度です。本制度では政府に登録された第三者の監査機関により、組織のガバナンス、物理的な監査を含む各種の管理策の実施状況の確認を経て登録されるものであり、登録には年次の更新が求められます。

本経済安全保障推進法との関連において、次のように表明されています。

“特定重要設備は、他の事業者が提供するクラウドサービスを利用して構築されることも想定される。・クラウドサービスについては、政府が求めるセキュリティ要求を満たしたサービスを予め評価・登録する制度（ISMAP）が既に整備されているところ、事業者負担の軽減の観点から、ISMAP を取得しているものについては、当該制度において確認している事項等に係る情報の届出を省略することを可能とすることが適切であると考えられる。”

AWS を特定重要設備の構成設備としてご利用されるお客様は、AWS の ISMAP 登録に依拠することで、「導入等計画書」における評価項目のうち、「構成設備」に関連する事項を一部省略することが可能となります。

AWS の ISMAP 関連リソース

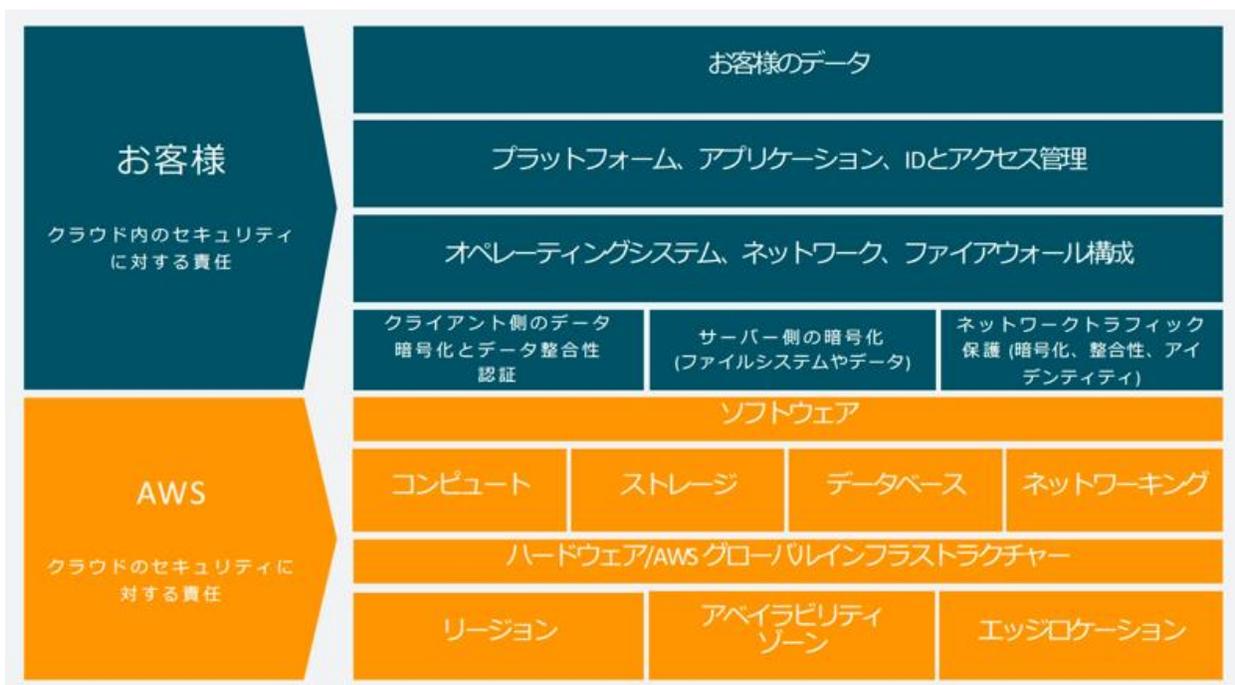
AWS の ISMAP ページ

<https://aws.amazon.com/jp/compliance/ismap/>

ISMAP Customer Package : AWS のコンプライアンスレポートにオンデマンドでアクセスできる無料のセルフサービスポータルである AWS Artifact から、ISMAP Customer Package が入手できます。

4 Amazon Web Services のシステムの概要

2006 年より、Amazon Web Services（AWS）は、高い柔軟性と拡張性を備えた安全な IT インフラストラクチャを世界中のあらゆる規模の企業に提供しています。AWS を利用することで、顧客はクラウドコンピューティング環境上でソリューションを展開し、ビジネスに必要な計算処理能力、ストレージ、その他のアプリケーションサービスをインターネット上で利用できるようになります。AWS では、任意のオペレーティングシステム、アプリケーションプログラム及びデータベースを柔軟に利用することができます。



上記図における「クラウドのセキュリティに対する責任」が本統制の責任範囲となります。AWS グローバルクラウドインフラストラクチャは、安全性、広範性、信頼性に最も優れたクラウドプラットフォームです。AWS は、処理やストレージなどさまざまな基本コンピューティングリソースをプロビジョニングするために使用するグローバルなクラウドインフラストラクチャを運用します。AWS グローバルインフラストラクチャには、施設、ネットワーク、ハードウェア、およびこれらのリソースのプロビジョニングと使用をサポートする運用ソフトウェア（ホスト OS、仮想化ソフトウェアなど）が含まれます。

お客様がリスク評価を行うために参考となる情報（特定重要設備の導入にあたって特定社会基盤事業者が講ずる特定妨害行為を防止するための措置に係る事項⑰に関連する情報）

お客様は本ドキュメントに基づき、特定重要設備の構成設備として AWS を利用する際のリスク評価を行う上での参考情報を確認することが出来ます。

AWS のお客様は、適用されるコンプライアンスに関する法律および規制に準拠する責任があります。場合によっては、お客様のコンプライアンスをサポートするために、AWS から機能（セキュリティ機能など）、支援ドキュメント、法的な契約書（AWS データ処理契約や事業提携契約など）が提供されます。

お客様がプライバシーとデータセキュリティについて懸念されるのは当然のことです。このため、AWS ではコンテンツの所有権と管理権をお客様にお渡ししています。シンプルかつパワフルなツールによって、自分のコンテンツをどこに保存するかをお客様に決定していただき、転送中のコンテンツと保管中のコンテンツを保護し、お客様のユーザーの AWS のサービスとリソースに対するアクセスを管理できるようにしています。また、お客様のコンテンツに対する不正アクセスや開示を防止するよう設計された、洗練された信頼性の高い技術的および物理的な管理を実践しています。

供給者の名称

アマゾン ウェブ サービス ジャパン合同会社(AWS Japan)

AWS のグローバルインフラストラクチャ（リージョン、アベイラビリティゾーンなど、関連する所在地）

AWS グローバルインフラストラクチャマップ

<https://aws.amazon.com/jp/about-aws/global-infrastructure/>

資本関係及び役員等の情報

お客様は Amazon.com, Inc.の Investor Relations より情報を参照することができます。

<https://ir.aboutamazon.com/overview/default.aspx>

必要な場合は AWS Japan の登記簿謄本を入手ください。

<https://www.touki-kyoutaku-online.moj.go.jp/>

事業計画や実績

お客様は Amazon.com, Inc.の Investor Relations より情報を参照することができます。

<https://ir.aboutamazon.com/overview/default.aspx>



設備又は部品を製造する工場等の所在地（お客様が構成設備として AWS サービスを選択する際の所在地等）

AWS グローバルインフラストラクチャマップ

<https://aws.amazon.com/jp/about-aws/global-infrastructure/>

作業に従事する者の所属・専門性

AWS コンプライアンスプログラムにより、セキュリティとクラウドのコンプライアンスを維持するために AWS に導入されている堅牢な管理について、お客様にご理解いただけます。ガバナンスに重点を置き、監査に適したサービス機能を該当するコンプライアンス規格または監査規格と結び付けることで、AWS コンプライアンスの実現を支援するドキュメントは、従来のプログラムに基づいて構築されており、お客様が AWS セキュリティ統制環境で確立し、運用するものとなっています。

作業に従事する要員の力量および継続的な教育の実施は ISO/IEC27001、ISMAP 管理基準その他の第三者評価により継続的に評価されています。

AWS コンプライアンスプログラム

<https://aws.amazon.com/jp/compliance/programs/>

5 AWS における経済安全保障推進法への対応

1. お客様が実施すべき事項

お客様は、お客様自身、お客様の契約した特定重要設備の供給者（特定重要設備の開発や運用、保守を担う事業者）、AWS を含む構成設備の供給者の役割と責任範囲に基づき、「導入等計画書」における評価を行い、監督官庁に提出する必要があります。

2. 「導入等計画書」4. 構成設備に関する事項

AWS は ISMAP 登録しているため、「4. 構成設備に関する事項」の（3）から（6）の記載は省略することができます。詳細は本ドキュメント 3.「AWS の ISMAP 関連リソース」をご参照ください。

3. 「導入等計画書」5. 特定重要設備の導入にあたって特定社会基盤事業者が講ずる特定妨害行為を防止するための措置に係る事項（共通項目）に関する考慮事項（共通項目）

下記記載の項目は構成設備としての AWS に係る範囲の確認、およびお客様の責任範囲に対する情報の提供として活用することが出来ます。また、お客様の責任範囲として、特定重要設備に係る項目に関しては、お客様が AWS 上で適切な設計及び運用を行うことが求められます。

なお、下記項目は、金融庁命令「様式第四（一）（第九条第一項関係） 導入等計画書（特定重要設備の導入を行う場合）」を参照しています。

<https://www.fsa.go.jp/news/r5/sonota/20230915/04.pdf>

規制業種ごとの個別要求事項は本ドキュメント 5.3 をご参照ください。

番号	項目	対象	ISMAP における 届出省略 項目	考慮事項	お客様のワークロードを支援するための AWS のサービス情報
(1) ①-1	特定重要設備への脆弱性テストの実施	特定重要設備		お客様のコンテンツを含むクラウド内のセキュリティについては、お客様が適切な安全管理措置を行う必要があります。	<p>Amazon Inspector は、ソフトウェアの脆弱性や意図しないネットワークのエクスポージャーがないか継続的に AWS ワークロードをスキャンする自動脆弱性管理サービスです。</p> <p>AWS Security Hub は、セキュリティのベストプラクティスのチェックを行い、アラートを集約し、自動修復を可能にするクラウドセキュリティ体制管理サービスです</p> <p>AWS Config は、AWS、オンプレミス、その他のクラウド上のリソースの設定と関係を継続的に評価、監査、評価します。</p>
①-2	構成設備における脆弱性テスト	構成設備	○	AWS は ISMAP サービスリストに登録されており、本統制を評価されています。	
②-1	特定重要設備への情報セキュリティ	特定重要設備		お客様のコンテンツを含むクラウド内のセキュリティについては、お客様が適切な安全管理措置を行う必要があります。	<p>Amazon Inspector は、ソフトウェアの脆弱性や意図しないネットワークのエクスポージャーがないか継続的に AWS ワークロードをスキャンする自動脆弱性管理サービスです。</p>

	要件の適用				<p>AWS Security Hub は、セキュリティのベストプラクティスのチェックを行い、アラートを集約し、自動修復を可能にするクラウドセキュリティ体制管理サービスです。</p> <p>AWS Well-Architected は、クラウドアーキテクトがさまざまなアプリケーションやワークロード向けに高い安全性、性能、障害耐性、効率性を備えたインフラストラクチャを構築する際に役立ちます。AWS Well-Architected では、6 つの柱（優れた運用効率、セキュリティ、信頼性、パフォーマンス効率、コストの最適化、持続可能性）に基づいて、お客様とパートナーがアーキテクチャを評価し、スケーラブルな設計を実装するための一貫したアプローチを提供しています。</p> <p>AWS Well-Architected Framework には、ドメイン固有のレンズやハンズオンラボ、そして AWS Well-Architected Tool が含まれています。追加コストなしで AWS マネジメントコンソールで利用できる AWS Well-Architected Tool は、ワークロードの定期的な評価、リスクの高い問題の識別、向上の記録を行うメカニズムを提供します。</p>
②-2	構成設備における情報セキュリティ	構成設備	○	AWS は ISMAP サービスリストに登録されており、本統制を評価されています。	

	要件の適用			
③-1	特定重要設備の開発工程における品質保証体制の確立	特定重要設備		<p>お客様のコンテンツを含むクラウド内のセキュリティについては、お客様が適切な安全管理措置を行う必要があります。</p> <p>Amazon CodeGuru セキュリティ は、機械学習 (ML) と自動推論を組み合わせた静的アプリケーションセキュリティ検査 (SAST) ツールです。コードの脆弱性を特定し、特定された脆弱性を修正する方法に関する推奨事項を提示し、終了するまで脆弱性のステータスを追跡します。詳細はこちら »</p> <p>Amazon CodeGuru Profiler を使用することで、デベロッパーは、アプリケーションのランタイム動作の理解、コードの非効率性の特定と除去、パフォーマンス向上、コンピューティングコストの大幅な削減を実現できます。これにより、アプリケーションの最もコストのかかるコード行を特定することができます。</p>
③-2	構成設備の開発工程における品質保証体制の確立	構成設備	○	<p>AWS は ISMAP サービスリストに登録されており、本統制を評価されています。</p>
④-1	特定重要設備における変更管理（不	特定重要設備		<p>お客様のコンテンツを含むクラウド内のセキュリティについては、お客様が適切な安全管理措置を行う必要があります。</p> <p>AWS CloudTrail は、AWS インフラストラクチャ全体のアカウントアクティビティをモニタリングして記録し、スト</p>

	正な変更の確認)				レンジ、分析、および修復アクションをコントロールできます AWS Config は、AWS、オンプレミス、その他のクラウド上のリソースの設定と関係を継続的に評価、監査、評価します。
④-2	構成設備における変更管理（不正な変更の確認)	構成設備	○	AWS は ISMAP サービスリストに登録されており、本統制を評価されています。	
⑤-1	特定重要設備における重要アクセス管理	特定重要設備		お客様のコンテンツを含むクラウド内のセキュリティについては、お客様が適切な安全管理措置を行う必要があります。	AWS Organizations は、AWS リソースの増加とスケールに合わせて、一元化されたクラウドアカウント管理を可能にします。 AWS Identity and Access Management (IAM) を使用すると、AWS のサービスやリソースにアクセスできるユーザーやグループを指定し、きめ細かいアクセス許可を一元管理し、アクセスを分析して AWS 全体でアクセス許可を改善することができます。
⑤-2	構成設備におけるアクセス管理	構成設備	○	AWS は ISMAP サービスリストに登録されており、本統制を評価されています。	AWS IAM アイデンティティセンター は、従業員 ID を安全に作成または接続し、AWS アカウントとアプリケーション全体の従業員アクセスを一元的に管理するのに役立ちます。IAM

					<p>アイデンティティセンターは、組織の規模や種類を問わず、AWS で従業員の認証と認可を行うための推奨されるアプローチです。IAM アイデンティティセンターを使用すると、AWS でユーザー ID を作成および管理したり、Microsoft Active Directory、Okta、Ping Identity、JumpCloud、Google Workspace、および Microsoft Entra ID (旧 Azure AD) などの既存の ID ソースを接続したりできます。</p>
⑥	<p>特定重要設備がインターネット接続を行う上でのセキュリティおよびマニュアル等の整備</p>	<p>特定重要設備</p>		<p>お客様のコンテンツを含むクラウド内のセキュリティについては、お客様が適切な安全管理措置を行う必要があります。</p>	<p>Amazon Virtual Private Cloud (Amazon VPC) は、リソースの配置、接続性、セキュリティなど、仮想ネットワーク環境をフルで制御できるサービスです。</p> <p>AWS WAF は、可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性のある一般的なウェブエクスプロイトやボットから保護するのに役立ちます。</p> <p>AWS Shield はマネージド型のDDoS 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。</p> <p>AWS WAF は、可用性に影響を与えたり、セキュリティを侵害したり、リソースを過剰に消費したりする可能性のある一般的なウェブエクスプロイトやボットから保護するのに役立ちます。</p>

⑦	特定重要設備の設置における不正な変更の防止	特定重要設備		お客様のコンテンツを含むクラウド内のセキュリティについては、お客様が適切な安全管理措置を行う必要があります。	<p>AWS CloudFormation は、インフラストラクチャをコードとして扱うことで、AWS およびサードパーティーのリソースをモデル化、プロビジョニング、管理することができます。</p> <p>AWS Control Tower は、組織のセキュリティとコンプライアンスのニーズを維持しながら、お客様に代わって複数の AWS サービスを調整します。</p> <p>AWS Identity and Access Management (IAM) を使用すると、AWS のサービスやリソースにアクセスできるユーザーやグループを指定し、きめ細かいアクセス許可を一元管理し、アクセスを分析して AWS 全体でアクセス許可を改善することができます。</p>
⑧-1	特定重要設備の導入後の不正な変更の防止	特定重要設備		お客様のコンテンツを含むクラウド内のセキュリティについては、お客様が適切な安全管理措置を行う必要があります。	<p>AWS Config は、AWS、オンプレミス、その他のクラウド上のリソースの設定と関係を継続的に評価、監査、評価します。</p> <p>AWS Systems Manager は、AWS 上およびマルチクラウドやハイブリッド環境内のリソースのための安全なエンドツーエンドの管理ソリューションです。</p> <p>AWS Security Hub は、セキュリティのベストプラクティスのチェックを行い、アラートを集約し、自動修復を可</p>

					能にするクラウドセキュリティ体制管理サービスです
⑧-2	構成設備における不正対応への協力	構成設備	○	AWS は ISMAP サービスリストに登録されており、本統制を評価されています。	
(2) ⑨-1	特定重要設備に対するサービス保証	特定重要設備		お客様のコンテンツを含むクラウド内のセキュリティについては、お客様が適切な安全管理措置を行う必要があります。	AWS は、クラウドプロバイダーの中で最高のネットワーク可用性を提供しています。各リージョンは完全に分離されており、インフラストラクチャの完全に分離されたパーティションである複数の AZ で構成されています。効果的に問題を隔離して、高可用性を実現するために、アプリケーションを同じリージョンにある複数の AZ で分離できます。 企業は必要に応じて迅速にリソースを増やすことができ、数百から数千ものサーバーを数分でデプロイできます。
⑨-2	構成設備に関するサービス保証の確認	構成設備	○	AWS は ISMAP サービスリストに登録されており、本統制を評価されています。	
⑩-1	特定重要設備の供給者によるサービス	特定重要設備		お客様のコンテンツを含むクラウド内のセキュリティについては、お客様が適切な安全管理措置を行う必要があります。	単一の AWS リージョン内にあるマルチ AZ 構成で充足が難しい災害や障害発生時の業務継続性要件が求められるワークロードやアプリケーション

	ス保証 が受け られない 場合 の代替 考慮事 項				を日本国内にある 2 つのリージョンの 連携により実現することが可能です。
⑩-2	構成設 備の供 給者に よるサー ビス保 証が受 けられ ない場 合の代 替考慮 事項	構成 設備	○	AWS は ISMAP サービスリストに登録さ れており、本統制を評価されています。	
⑪ (3)	特定重 要設備 における ランサム ウェア等 への事 業継続 体制の 設備	特定 重要 設備		お客様のコンテンツを含むクラウド内のセキ ュリティについては、お客様が適切な安全 管理措置を行う必要があります。	AWS の eBook「ランサムウェアから AWS 環境を守る」では、どのような機 関がリスクにさらされるのか、なぜランサ ムウェアが有効な攻撃となってしまうの か、身代金を払うべきか払わないべき か、そして、AWS 上で構築することで 顧客が特定のセキュリティコントロール を自動的に継承できる方法について 紹介しています。AWS クラウド上で 構築する場合には、インシデント発生 前、発生中、発生後のランサムウェア 対策能力を強化するために適用でき る重要なセキュリティの観点とサービス があります。

⑫	特定重要設備におけるセキュリティインシデントへの対応体制の整備	特定重要設備		お客様のコンテンツを含むクラウド内のセキュリティについては、お客様が適切な安全管理措置を行う必要があります。	AWS セキュリティインシデント対応ガイド このガイドでは、お客様の AWS クラウド環境におけるセキュリティインシデント対応の基礎について概要を提供します。クラウドセキュリティとインシデント対応の概念に注目し、お客様がセキュリティ問題に対応する際に利用できるクラウドの機能、サービス、メカニズムについて説明します。
⑬	特定重要設備への不正アクセス管理体制の整備	特定重要設備		お客様のコンテンツを含むクラウド内のセキュリティについては、お客様が適切な安全管理措置を行う必要があります。	お客様の組織的要件となります。
(4) ⑭-1	特定重要設備における法令遵守	特定重要設備		お客様のコンテンツを含むクラウド内のセキュリティについては、適切な安全管理措置を行う必要があります。	お客様の組織的要件となります。
⑭-2	構成設備における法令遵守	構成設備	(直接報告)	本文書は、バイパス制度に基づき、以下の省庁に直接提出を行う予定です。対応が必要な場合は、弊社アカウントチームにご連絡ください。	
(5) ⑮-1	特定重要設備における外国の法的環	特定重要設備		お客様のコンテンツを含むクラウド内のセキュリティについては、お客様が適切な安全管理措置を行う必要があります。	お客様の組織的要件となります。

	境や外部主体の指示に対する報告				
⑮-2	構成設備における外国の法的環境や外部主体の指示に対する報告	構成設備	(直接報告)	本文書は、バイパス制度に基づき、以下の省庁に直接提出を行う予定です。対応が必要な場合は、弊社アカウントチームにご連絡ください。	
⑯	特定重要設備を設置する場合における映像情報の取り扱いの適切性	特定重要設備			<p>Amazon Simple Storage Service (Amazon S3) は、業界随一のスケーラビリティ、データ可用性、セキュリティ、パフォーマンスを提供するオブジェクトストレージサービスです。あらゆる規模や業種のお客様が、データレイク、クラウドネイティブアプリケーション、モバイルアプリケーションなど、事実上あらゆるユースケースで、あらゆる量のデータを保存、保護することができます。コストパフォーマンスに優れたストレージクラスと使いやすい管理機能により、コストの最適化、データの整理、特定のビジネス、組織、コンプライアンスの要件を満たすきめ細かなアクセスコントロールの設定を行うことができます。</p>

					<p>S3 Glacier のボールドロックでは、ボールドロックポリシーを使用して、S3 Glacier の各ボールドに対するコンプライアンス管理を簡単にデプロイして適用することができます。ボールドロックポリシーで「write once read many」(WORM) などの管理を指定してポリシーをロックし、今後編集できないようにします。</p>
<p>(6) ⑰</p>	<p>特定重要設備及び構成設備の供給者に関する情報提供</p>	<p>特定重要設備および構成設備</p>		<p>本ドキュメント4. をご参照ください。</p>	

4. その他規制業種毎の個別要求項目

電力：⑰が“核原料物質、核燃料物資及び原子炉の規制に関する法律に従い、当該情報システムによる当該操作の適切性が影響を受けないことを確認していること”が追加要求となる

<https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000259688>

対応：

AWS の SOC 2 レポートは AWS の統制環境に関する説明と AICPA の信頼サービスのセキュリティ、可用性、機密性、プライバシーの基準を満たす AWS 統制の外部監査に関する説明を提供しています。

Document Revisions

Date	Description
Sep 30 2023	第 0.1 版発行 9 月 15 日の発行情報にあわせて
Feb 01 2024	第 1.0 版発行
Apr 12 2024	第 1.1 版発行 バイパス制度への言及
May17 2024	第 1.2 版発行