北米電力信頼度協議会 重要インフラ保護基準 (NERC CIP) 対応のための AWS ユーザーガイド

2021 年 11 月

注意

お客様は、本書に記載されている情報を独自に評価する責任を負うものとします。本書は、(a) 情報提供のみを目的としており、(b) AWS の現行製品とプラクティスを表したものであり、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、またはライセンサーからの契約義務や確約を意味するものではありません。AWS の製品やサービスは、明示または暗示を問わず、いかなる保証、表明、条件を伴うことなく「現状のまま」提供されます。お客様に対する AWS の責任は、AWS 契約により規定されます。本書は、AWS とお客様の間で行われるいかなる契約の一部でもなく、そのような契約の内容を変更するものでもありません。

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.

目次

クラウド「の」セキュリティ (AWS の責任) 6

コンプライアンスプログラム 7

クラウド「内」のセキュリティ (電力事業者の責任) 11

統制の継承 12

電力事業者向けのリソース 14

AWS のインフラストラクチャ 16

自動化 17

大規模環境でのガバナンス 18

ID とアクセスの管理 22

データ保護 23

論理的な分離とセキュアなネットワーク 26

設定、脆弱性、パッチ管理 28

セキュリティイベントの監視活動 29

インシデント対応 31

レジリエンスとシステム復旧 32

リモート、エッジ、オンプレミスコンピューティング 33

物理的セキュリティ 35

このガイドについて

本書では、NERC に所属する電力事業者が、AWS のサービスを使ってクラウドテクノロジーによるメリットを実現するとともに、北米電力信頼度協議会（NERC、North American Electric Reliability Corporation）重要インフラ保護基準（CIP、Critical Infrastructure Protection）で求められているコンプライアンス要件に対応する方法を解説します。また、NERC CIP の目的に合致するクラウドセキュリティの中心的概念について説明し、AWS のサービスが NERC CIP の要件にどのように適合しているかを示します。さらに、NERC に所属する電力事業者が AWS クラウドへの移行を計画するための方法についても考察します。

概要

本書では、安全性および信頼性に優れたインフラストラクチャを AWS がどのように提供しているかを示すとともに、幅広い AWS クラウドサービスを使用して NERC CIP 標準のセキュリティ目標と信頼性目標をサポートする方法について説明します。以下の各セクションでは、各電力事業者が NERC CIP 標準に準拠してその状態を維持するための AWS のサービスに関する情報、これらのサービスが NERC CIP 標準に適合している根拠、規制範囲内でデータとシステムに AWS クラウドサービスの使用を計画する電力事業者のための考慮事項について説明します。

背景

AWS では、電力とエネルギー分野のお客様が、ビジネス目標の達成と顧客ニーズへの対応を目的としたクラウドコンピューティングテクノロジーの活用に興味をお持ちであると認識しています。電力網の運営環境は、分散化と脱炭素化の傾向によって変化しつつあります。信頼性の高い運営を維持するために業界で行われている変革的対応の重要な部分に、クラウドソリューションが位置付けられています。IDC は次のように指摘しています。

> 「電力とエネルギー分野でのデジタル化が進む中、クラウドを利用した製品およびサービスは、拡張性と安全性に優れたデータストレージをオンデマンドアクセスで提供しつつ IT とインフラストラクチャの全体的なコストを削減するための魅力的なオプションを企業に提供しています。」

仮想化やクラウドコンピューティングなどの分野でのテクノロジーの進化に伴い、責任主体がオペレーション面、セキュリティ面、レジリエンス面の目標を達成するために新しいテクノロジーを使用できるように、電力事業者、規制当局、サービスプロバイダーによる取り組みが行われています。例えば規制当局は、クラウドテクノロジーに

よって生じる多様な機会を認識しています。規制当局は、クラウドの導入そのものや、規制に準拠して安全にクラウドを導入できるように電力事業者を支援することを目的とし、自らの役割を明確化するために前進しています。連邦エネルギー規制委員会 (FERC、Federal Energy Regulatory Commission) のクラウドコンピューティングに関する情報請求告示 (NOI、Notice of Inquiry) への対応として、NERC では次のように述べています。

> 「*ERO Enterprise* では、*BCSI* のデータストレージとしてクラウドコンピューティングの使用をサポートしています。これは、データストレージのサードパーティサービスによって生じるリスクを適切に軽減できるためです。*...ERO Enterprise* ではさらに、*BES* の信頼性運用サービスについても、リスクと脆弱性を軽減するために適切な保護が実施されていればクラウドコンピューティングの使用をサポートできます。」

米国の電力セクターは、連邦の独立機関である FERC によって管理されています。FERC は、液化天然ガス、石油、電力の州間送電とともに、天然ガスと水力発電プロジェクトを管理しています。大規模電力システム (BES: Bulk Electric System) の信頼性を保護するために、米国電力セクターの電力事業者には、法的強制力のある必須のセキュリティ要件が適用されます。

2006 年、FERC は北米電力信頼度協議会 (NERC、North American Electric Reliability Corporation) に、電力信頼度機関 (ERO、Electric Reliability Organization) として重要インフラストラクチャ保護 (CIP、Critical Infrastructure Protection) のサイバーセキュリティ信頼性基準を策定する権限を認定しました。この基準は、電力網の計画と運営に関するセキュリティと信頼性を確保するために策定されるものです。大規模電力システムについて定義されている設備または業務の範囲に適合する電力事業者は、NERC CIP 標準の範囲に含まれるデータ、設備、システムについて、この標準に準拠することが義務付けられています。

FERC は複数の信頼性技術会議 (Reliability Technical Conference) を通じ、エネルギー供給の計画と運営にクラウド環境の利点を安全かつ効果的に活用するには、どのように標準を展開すべきかについて議論を進めました。

FERC スタッフレポート、FERC 委員会オープン会議、2019 年 11 月 21 日

クラウド/マネージドセキュリティサービスプロバイダー: この重点分野では、電力事業者がクラウドおよびマネージドセキュリティサービスプロバイダーのデプロイ方法を検討する場合に、安全な方法でのデプロイが重要であると認識されています。適切に実施されれば、信頼できるサードパーティに一般的なタスクやサービスを委託すると、電力事業者が社内のより複雑な問題に専念してセキュリティリソースを最適化できるため、セキュリティ上の利点が得られます。ただし、リアルタイム運用で使用されるシステムなど、きわめて重要性の高いシステムをクラウドで運用できるかどうかを判断するには、さらに調査が必要です。

続いて 2020 年 2 月、仮想化とクラウドコンピューティングに関する情報請求告示により、関心を持つ利害関係者や業界団体からパブリックコメントを収集しました。さらに 2020 年末、FERC は NERC に対し、仮想化とコンピューティングの使用の潜在的な利点とリスクについて、2021 年末までに情報をまとめて提出するよう指示しました。

「仮想化とクラウドコンピューティングの自発的な使用は、これらのテクノロジーに関連するリスクへの対処が慎重に行われる限り、大容量電力システムのユーザー、所有者、運用者に大きなメリットをもたらす可能性があるという点で、NOI のコメントは概ね一致しています。」

クラウド導入について理解しサポートするという作業は CIP 立案チームの業務の一環です。このチームでは、標準開発プロセスに従い、必要に応じて文言改訂の評価と提案を

行っています。業界では、改訂要件に先立ち、クラウド上の BES サイバーシステム情報 (BCSI) の評価を行う CIP 監査人を支援する NERC 実践ガイダンスに準拠するように、クラウド上の BCSI の利用を可能にする方法を明確にした CIP-004 および CIP-011 の改定を承認しました。改訂は FERC による承認待ちの段階です。また、CIP-004-6 と CIP-011-2 では、クラウドソリューションや BCSI の暗号化に関する実装ガイダンスが提案されています。

技術的な利害関係者の作業グループが、要件の文言と根拠を示す義務についてクラウドサービスの使用を評価し、電力事業者がクラウドサービスを使用する際に CIP 標準への準拠を実証する方法を示したガイダンスを作成しています。2019 年 6 月、NERC は、リスクの特定と評価のために許容できる手段として、サードパーティの独立した評価を使用するためのガイダンスを承認しました。(NATF CIP-013-1 実装ガイダンスを参照してください)

セキュリティ、責任共有、統制の継承

クラウドのセキュリティは共有責任です。責任共有モデルは、クラウドセキュリティ原則のコンテキストにおいて、電力事業者と AWS のそれぞれの役割を理解するうえで重要になります。AWS は、AWS クラウドで提供されるあらゆるサービスの実行基盤となるインフラストラクチャを保護する責任があります。このインフラストラクチャは、AWS クラウドサービスを実行するハードウェア、ソフトウェア、ネットワーク、施設から成り立っています。電力事業者は、クラウド上にある自社のデータとシステムに関するセキュリティについて責任を負います。つまり電力事業者には、自社のコンテンツ、アプリケーション、システム、ネットワークを保護するためにどのようなセキュリティプログラムを実装するかについて主導権があるということです。これは、オンサイトのデータセンターで使用するアプリケーションに関する主導権とまったく同じです。

AWS は、ホストオペレーティングシステムや仮想化レイヤーから、サービスが運用される施設の物理的セキュリティまで、IT コンポーネントの運用、管理、制御を行います。

責任の境界線は、クラウドワークロードでどの機能を実行し、どのサービスを選択するかによって異なります。電力事業者と AWS の間でどのような責任分担になるかを理解することは、クラウド導入プロセスの重要な部分です。電力事業者がクラウド環境のサポートに他のサードパーティソリューションを活用する場合、サードパーティと電力事業者間の責任共有モデルは AWS 責任共有モデルと異なることがあり、電力事業者のセキュリティ責任が増える可能性がある点を考慮する必要があります。

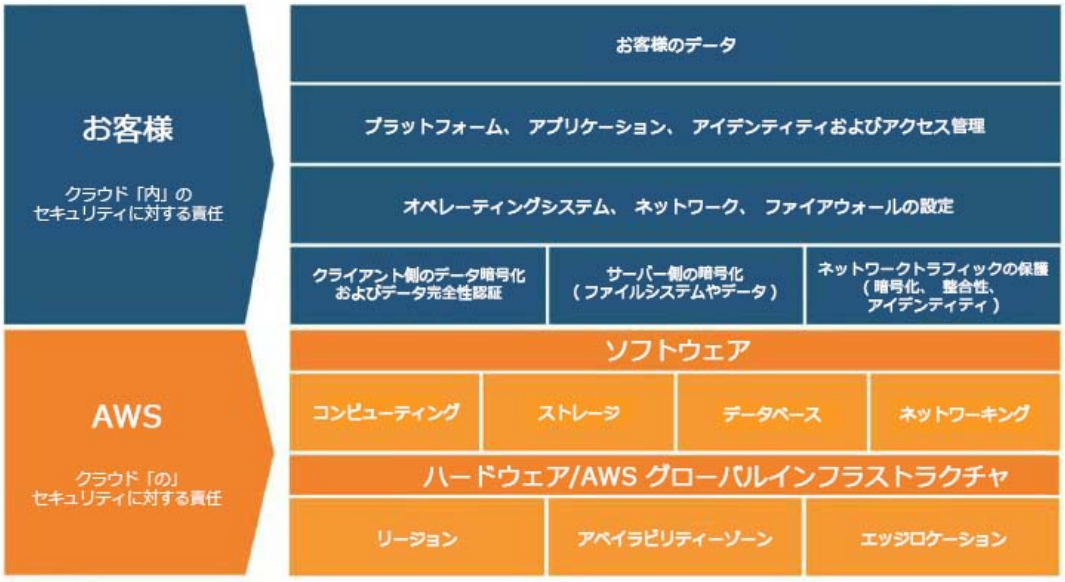

図 1: 責任共有モデル

CIP への準拠を達成するうえで、NERC CIP 標準への準拠を確認する責任は電力事業者が負います。電力事業者は、NERC CIP で分類されている設備に適用可能なファイアウォール設定やネットワークトラフィック保護統制など、CIP 要件を満たすセキュリティ統制を管理します。AWS は、AWS データセンターへの物理アクセス制御など、クラウドインフラストラクチャに対する統制を管理します。セキュリティ統制活動を実行する責任は、電力事業者と AWS が共有します。

クラウド「の」セキュリティ (AWS の責任)

クラウドのセキュリティを提供するために、AWS の環境は継続的に監査されます。インフラストラクチャとサービスは、「コンプライアンスプログラム」のセクションで説明しているように、複数の地域や業界にわたって指定のコンプライアンス基準および業界認証の下で運用されていることが承認されています。電力事業者はこれらの認証を使用して、国際的に認知されているセキュリティのベストプラクティスや認証など、AWS のセキュリティ統制の実装と有効性を検証できます。AWS コンプライアンスプログラムは、以下のアクションに基づいています。

- **検証**: 世界中で AWS サービスと施設がさまざまな統制環境に準拠し、効果的に運用されていることを検証します。AWS の統制環境には、ポリシー、プロセス、統制活動が含まれており、これらには AWS の全体的な統制環境のさまざまな面が利用されています。この全体的な統制環境には、統制フレームワークの効率的な運用を支える環境を構築し維持するために必要な人員、プロセス、テクノロジーが含まれています。AWS は、クラウドコンピューティング業界の主要機関によって定義されたクラウド固有の統制について、該当する項目を AWS の統制フレームワークに統合しました。実装可能な優れたプラクティスを定義し、統制環境の管理にさらに役立つことができるように、AWS ではこのような業界団体の動きに注目しています。
- **開示**: お客様が業界や政府の要求事項へのコンプライアンス対応状況を検証できるよう、AWS ではコンプライアンス対応の方針を開示しています。AWS は外部の認定機関および独立監査人と協力し、AWS が規定および運用しているポリシー、プロセス、統制に関する重要な情報をお客様に提供しています。お客様はこの情報を活用して、統制の評価と検証の手順を実行できます。
- **監視活動**: AWS はセキュリティで保護された安全な環境を提供し、お客様がインフラストラクチャを保護できるように数千ものセキュリティ統制要件を通じて支援しています。

コンプライアンスプログラム

お客様は、AWS コンプライアンスプログラムを参照すると、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理解することができます。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、運用することができるようになっています。

AWS が順守する IT 標準は、認証と証明、法律と規制、プライバシー、準拠とフレームワークに分類されます。コンプライアンス認証と証明は、サードパーティである独立監査人によって監査され、その結果としてコンプライアンス認証、監査報告、または証明が発行されます。AWS のお客様は、適用可能なコンプライアンスに関する法律、規制、プライバシープログラムに準拠する責任があります。コンプライアンスへの準拠とフレームワークには、特定の業界または機能など、特定の目的のために公開されたセキュリティまたはコンプライアンス要件が含まれます。

AWS では、他よりも多くのセキュリティ規格やコンプライアンス認証 (PCI-DSS、HIPAA/HITECH、FedRAMP、GDPR、FIPS 140-2、NIST 800-171 を含む) をサポートしているため、お客様は世界中のほぼすべての規制機関によるコンプライアンス要件を満たすことができます。

AWS Artifact

AWS Artifact とは、AWS マネジメントコンソールで利用できるセルフサービスの監査報告レポート取得ポータルです。お客様はこれを使用して、2,500 を超えるセキュリティ統制に関するレポートと詳細をオンデマンドで確認およびダウンロードできます。

これらのセキュリティ保証プログラムで求められる統制のベースとなるセキュリティ目標は、CIP セキュリティ目標と合致するものであり、定期的にクラウドセキュリティの専門家によって厳格な監査と認定を受けています。電力事業者は、クラウドインフラストラクチャの CIP セキュリティ目標を達成するために、AWS が管理する統制を継承し、ユーザーによるクラウド環境の保護に役立つ AWS ツールを活用します。

NERC の規制対象となる電力事業者にとって特に役立つ保証プログラムには、次のようなものがあります。

- **FedRAMP** – セキュリティ評価、認証、継続的な監視活動に関する規格を統一するための米国政府プログラムです。AWS は FedRAMP に準拠したサービスを提供しています。これらは、「高」または「中」の影響レベルの認可を受けており、認定済みの独立した第三者評価機関 (3PAO、Third-Party Assessment Organization) によって評価され、FedRAMP の継続的な監視要件を維持しています。継続的な監視要件は、米国国立標準技術研究所特別刊行物 (NIST SP、National Institute of Standards and Technology Special Publication) 800-137 「連邦情報システムおよび組織の情報セキュリティ継続監視」 (Information Security Continuous Monitoring for Federal Information Systems and Organizations) に基づいており、これについては FedRAMP 継続的モニタリング戦略ガイド (FedRAMP Continuous Monitoring Strategy Guide) で解説されています。AWS リージョンは FedRAMP 認証を受けています (AWS East-West リージョンを構成する 4 つのリージョンは FedRAMP 「中」レベル、2 つの

GovCloud リージョンは FedRAMP の「高」レベルです)。承認された AWS サービスは、FedRAMP Marketplace で AWS のサービス説明の下に掲載されています。

- **SOC** – AWS Service Organization Control (SOC) レポートは、重要なコンプライアンスの統制および目標に AWS がどのように取り組んだかを実証する、独立したサードパーティによる審査報告書です。これらのレポートは、お客様による運用とコンプライアンスをサポートするために確立された AWS の統制について、電力事業者と監査人が理解することを目的としています。AWS の SOC 1、SOC 2、SOC 3 レポートは、6 か月間をレポート対象として年に 2 度発行されます。新レポートは、5 月中旬と 11 月中旬にリリースされます。

  AWS SOC レポートには、次の 3 種類があります。

  - **SOC 1** – AWS の統制環境に関する情報を提供します。この情報は、財務報告に係るお客様の内部統制に直結する可能性があり、財務報告に係る内部統制 (ICOFR、Internal Control over Financial Reporting) の有効性に関する評価および意見を求めるための情報としても使用されます。
  - **SOC 2** – システムのセキュリティ、可用性、機密性に関連する AWS の統制環境について、ビジネスニーズのあるお客様およびそのお客様のサービスユーザーに、独立した評価を提供します。
  - **SOC 3** – システムのセキュリティ、可用性、機密性に関連する AWS の統制環境について、ビジネスニーズのあるお客様およびそのお客様のサービスユーザーに、独立した評価を提供します。AWS の内部情報は開示されません。
- **ISO 27001** – ISO 27001 は、ISO 27002 のベストプラクティスガイダンスに従い、セキュリティ管理のベストプラクティスと包括的なセキュリティ統制を規定したセキュリティ管理標準です。この認証の基礎は強固なセキュリティプログラムの開発と実装であり、これには、AWS がどのようにしてセキュリティを全体的で包括的な方法で永続

的に管理するかを定義する、情報セキュリティ管理システムの開発と実装が含まれます。

- **ISO 27017** – ISO 27017 では、クラウドコンピューティングの情報セキュリティに関するガイダンスを提供し、ISO 27002 と ISO 27001 の規格のガイダンスを補完する、クラウド固有の情報セキュリティ統制の実装を推奨しています。この実施基準により、クラウドサービスプロバイダーに固有の、情報セキュリティ統制および実装ガイダンスが追加されます。
- **ISO 27018** – ISO 27018 は、クラウド内での個人データの保護に焦点を当てた実施基準です。ISO 情報セキュリティ規格 27002 に基づいており、パブリッククラウド内の個人を特定できる情報 (PII) に適用される ISO 27002 制御の実装ガイダンスを提供しています。また、既存の ISO 27002 統制セットでは扱われていないパブリッククラウド PII 保護要件を扱う追加統制セットと、それに関連するガイダンスも提供しています。
- **NIST サイバーセキュリティフレームワーク** – AWS などのクラウドサービスプロバイダーの評価、従来のテクノロジー購入の優先順位の確立、人員とスキルにおける不足部分の特定など、CSF は組織全体のセキュリティとコンプライアンスの目標を達成するための共通の基盤として使用できます。多くのテクノロジープロバイダーは、既にサービスや製品を NIST CSF にマッピングして、評価、取得、準拠のプロセスを合理化し、低コストで実現しています。

AWS は、SOC 1、2、3、FedRAMP の「中」または「高」など、複数のセキュリティ規格に準拠しています。これらを含めた多数のコンプライアンスプログラムの一環として、AWS データセンターのセキュリティの再調査および監査が行われます。お客様は **AWS マネジメントコンソール**にサインインして **Artifact** に移動することで、これらのコンプライアンスプログラムに関連付けられた監査レポートをダウンロードできます。これらの監査レポートは、規格への準拠または要件達成の証拠として、お客様の監査人に提示できます。

電力事業者のコンプライアンスチームは、AWS 認定、証明、監査基準を自社の監査プログラムに組み込み、要件への準拠に役立てることができます。AWS からの認定と証明の詳細については、AWS コンプライアンスセンターを参照してください。

クラウド「内」のセキュリティ (電力事業者の責任)

電力事業者は、クラウド「**内**」のセキュリティと、規制対象となるシステムのセキュリティ確保に責任を負います。これには、ゲストオペレーティングシステムの管理 (更新プログラムやセキュリティパッチのインストールなど) や、その他の関連するアプリケーションソフトウェアの管理のほか、AWS から提供されるセキュリティグループファイアウォールの設定が含まれます。例えば、クラウドで管理されるシステムのアカウント設定、管理、見直しの要件を満たすために、電力事業者は AWS Identity and Access Management (IAM) などのサービスを使用して、ユーザーアクセスと権限を設定および管理できます。

電力事業者の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用法令に応じて異なるため、電力事業者は選択するサービスを注意深く検討する必要があります。電力事業者がクラウドサービスの選択と実装を行うには、利用可能な AWS リソースの使用をお勧めします (AWS Well-Architected フレームワークのセクションを参照してください)。

AWS のサービスを使用する場合、電力事業者は自社のコンテンツに対する統制権を保持し、以下を含めてセキュリティ統制の設定を管理する責任を負います。

- 電力事業者が使用する AWS のサービスとセキュリティ機能の選択。
- コンテンツの保管場所とする国。
- コンテンツの形式や構造と、コンテンツにマスク、匿名化、暗号化を適用するかどうか。
- データを保管中または転送中に暗号化するかどうかと、キーの管理方法。
- コンテンツへのアクセスを誰に許可するか、アクセス権限の付与、管理、取り消しをどのように行うか。
- 可用性要件を定義し、その要件に沿ってレジリエンスに優れたアーキテクチャを構築する。

NERC CIP 要件には、電力事業者固有のポリシー、計画、またはプロセスによって対処し、電力事業者で管理するものがあります。これに該当する要件として、CIP-002 のシステム分類プロセス、CIP-003 で求められる包括的なポリシー、CIP-008 のインシデント対応計画などがあります。このような統制のパフォーマンスをサポートするためにクラウドサービスを使用できますが、電力事業者はコンプライアンスプログラムに従って要件を満たし、必要に応じてクラウドサービスに合わせて管理ドキュメントを更新する必要があります。

統制の継承

電力事業者は、クラウドインフラストラクチャ「**の**」セキュリティを提供するための統制を継承できます。AWS のインフラストラクチャは、柔軟性と安全性に優れ、軍事、多国籍銀行、電力とエネルギー業界など機密性の高い組織のセキュリティ要件を満たせるように設計されています。前述のとおり、AWS のインフラストラクチャとサービ

スは、多数のセキュリティ保証プログラム内で具体化されている何千ものセキュリティ要件を満たし、監査と継続的な監視活動によって検証されます。AWS のすべてのお客様は、最高機密のワークロードに対する要件を満たしているものと同じ安全なハードウェアとソフトウェアを利用できます。

AWS にワークロードをデプロイすることによって電力事業者が継承する統制の例として、AWS がデータセンター向けに実装している物理アクセス制御の制限があります。IT インフラストラクチャコンポーネントを収容するすべての AWS データセンターへの物理的なアクセスは、業務を実行するためにアクセスを必要とする認定済みの人物 (データセンターの従業員、ベンダー、AWS の請負業者) に制限されます。施設への立ち入りは、統制されたアクセスポイントのみで許可されます。そこでは、テールゲーティングを防止し、承認された人物のみに AWS データセンターへの入館を許可するために設計された、多要素認証が求められます。AWS データセンターへのアクセス権を持つ要員のアクセスリストと認証情報は、各データセンターの Area Access Manager (AAM) が四半期ごとに確認します。さらに、クラウドコンピューティングの性質上、お客様のデータはデータセンター内の特定のサーバーに割り当てられず、不正な論理アクセスから保護され、物理的セキュリティが強化されます。

責任共有と統制の継承に関する詳細と、これらが CIP の標準と要件によってどのように適用されるかを示した表については、「付録: AWS のサービスと NERC CIP への適合」をご覧ください。

AWS は、技術文書、レポート、認証、その他のサードパーティによる証明を通じて、AWS の統制環境に関する幅広い情報をお客様に提供しています。本書は、お客様が使用する AWS の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ためのものです。また、この情報は、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、検証するためにも有用です。AWS インフラストラクチャとサービスを使用してセキュリティとコンプライ

アンスの目標を達成する方法の詳細については、「セキュリティ、アイデンティティ、コンプライアンスに関するベストプラクティス」をご覧ください。

電力事業者向けのリソース

電力事業者にはクラウド内のワークロードを保護する責任があり、AWS はニーズを満たす安全なクラウドアーキテクチャの設計に関するサポートと専門知識を提供しています。AWS では、電力事業者が NERC CIP のワークロード用にアーキテクチャとセキュリティ統制を決定するために役立つリソースをご用意しています。

AWS では、セキュリティと信頼性に関する目標を達成するための最適なアプローチを定義できるようにお客様を支援する目的で、Well-Architected フレームワークを開発しました。Well-Architected フレームワークは、運用上の優秀性、セキュリティ、信頼性、パフォーマンス効率、コスト最適化という 5 つの柱に基づいています。（訳注：2022年11月現在で、「持続可能性」の柱が追加され、6 つの柱となっています）これらの柱は、ワークロード間で標準化して適用できるアーキテクチャを電力事業者、お客様、パートナーが評価して実装するための一貫したアプローチを提供します。電力事業者は AWS Well-Architected ツールを使用してワークロードの状態を確認し、AWS アーキテクチャに関する最新のベストプラクティスと比較できます。AWS のソリューションアーキテクトは、電力事業者のビジネス目標、ワークロード、目標に合わせて改善を行うためのガイダンスを提供します。

AWS クラウド導入フレームワーク (AWS CAF) は、電力事業者が効率的かつ効果的なクラウド導入計画を策定して実行できるように設計されています。このフレームワークで提供しているガイダンスとベストプラクティスは、お客様が IT ライフサイクル全体にわたり、組織全体でクラウドコンピューティングへの包括的なアプローチを構築するために役立ちます。AWS CAF では、ガイダンスをパースペクティブと呼ばれる 6 つの重点分野に体系化しています。これらのパースペクティブには、機能的に関連するステークホルダーが所有または管理する明確な責任が織り込まれています。一般的に、

ビジネス、人員、ガバナンスのパースペクティブではビジネス遂行能力に焦点を当て、プラットフォーム、セキュリティ、オペレーションのパースペクティブでは技術的能力に焦点を当てています。AWS CAF では、複雑な計画プロセスを、管理可能な注力分野に分割します。

電力事業者は AWS セキュリティコンピテンシーパートナーと協力して、クラウドでのセキュリティの強化と拡張に取り組むこともできます。AWS セキュリティコンピテンシーパートナーは、さまざまなワークロードやユースケースで利用できるソリューションでデータを保護するための SaaS (Software-as-a-Service) 製品など、特定のワークロードやユースケース向けにセキュリティに重点を置いたソリューションの提供に特化しています。

AWS Well-Architected フレームワーク、AWS CAF、AWS セキュリティコンピテンシーパートナーのほかにも、お客様がクラウド導入過程で活用できる無料のリソースが多数用意されています。本書の「その他のリソース」セクションに記載されているホワイトペーパー、コンピュータベースのトレーニング、AWS Workshops などがあります。

セキュリティとコンプライアンスへの対応をサポートする統制の実装

AWS クラウドにソリューションを実装すると、電力事業者は、クラウドセキュリティの技術力によって構築され、拡張性とレジリエンスに優れたインフラストラクチャを手にできます。これにより、電力事業者は幅広いサービスとオートメーションを使用して、大規模なガバナンスの提供、セキュリティ機能の強化、コンプライアンス要件の実証を行い、信頼性を実現できます。

AWS のインフラストラクチャ

AWS グローバルクラウドインフラストラクチャは、安全性、拡張性、信頼性に優れ、世界各地のデータセンターから 200 を超えるフル機能のサービスを提供しています。これには北米の 7 つのリージョンが含まれ、そのうちの 2 つは米国の GovCloud リージョンです。AWS GovCloud (政府機関向けクラウド) は、連邦政府、州、および地方レベルの米国政府機関の特定の規制とコンプライアンス要件に対応するように設計および構築されています。AWS GovCloud リージョンは FedRAMP の「高」として認証を受けており、米国の国際武器取引規則 (ITAR、International Traffic in Arms Regulations)、国防総省 (DoD、Department of Defense) クラウドコンピューティングセキュリティ要件ガイド (SRG) 影響レベル 2、4、5 などの特定の規制とコンプライアンス要件にも準拠しています。米国の他のすべての AWS リージョンは、FedRAMP Moderate として承認されています。これらの各リージョンは、複数のデータセンターから成る複数のアベイラビリティーゾーンで構成されています。AWS のコアインフラストラクチャは、機密性の高い組織の要件に適合できるように構築されており、これと同じセキュアなハードウェアとソフトウェアを使用して、各リージョンが構築および運用されています。

AWS は、お客様のセキュリティニーズを念頭に置いて絶えず革新を続けています。AWS は、AWS Nitro を使用して、運営している仮想化インフラストラクチャを全面的に再構成しました。従来、ハイパーバイザーは、物理的なハードウェアと BIOS を保護し、CPU、ストレージ、ネットワークを仮想化し、数多くの管理機能を提供してきました。そこに Nitro System が加わったことで、AWS はそのような機能を分割し、専用のハードウェアとソフトウェアに負荷を分散して、サーバーのほぼすべてのリソースをお客様のインスタンスに割り当てることにより、コストを軽減できるようになりました。この Nitro System は、インスタンスのハードウェアとファームウェアを継続的に監視、保護、検証し、セキュリティを一層強化します。仮想化リソースの負荷が専用のハードウェアとソフトウェアに分散され、攻撃対象領域が最小化されます。さ

らに、Nitro System のセキュリティモデルはロックダウン型です。インスタンスへの管理者アクセスを禁止し、人的エラーや不正の可能性を排除します。

電力事業者は、信頼性と可用性に優れた設計のさまざまな AWS のサービスを使用して、さらに高い信頼性を確保できます。例えば Amazon S3 では、電力事業者が選択したリージョン内の複数のアベイラビリティーゾーンにわたって自動的にデータを保存することで、99.999999999% の耐久性を実現します。電力事業者は、信頼性をさらに強化するために、AWS KMS を使用してこのデータを暗号化し、別の北米リージョンにデータをレプリケートするように Amazon S3 を設定できます。AWS の Amazon Aurora は、MySQL および PostgreSQL と互換性のあるデータベースサービスであり、ユーザー設定に基づいてアベイラビリティーゾーンとリージョンの間でデータレプリケーションを行います。また、AWS で利用できる Amazon RDS は、MS SQL Server や Oracle などの一般的なリレーショナルデータベースを提供し、複数のアベイラビリティーゾーンにデータを保存できるサービスです。電力事業者は、地理的に分散したインフラストラクチャでサポートされている AWS のサービスを利用することで、可用性および信頼性に優れたシステムを構築できます。

自動化

クラウドサービスを使用することで、セキュリティのベストプラクティスを簡単に自動化できます。すべての AWS の機能とアクションには、アプリケーションプログラミングインターフェイス (API、Application Programming Interface) 経由でアクセスできます。API へのアクセスは、AWS Identity and Access Management (AWS IAM) サービスによって統制されます。これらの API により、電力事業者はクラウドネットワーク、セキュリティ、アクセス管理、サーバー、ストレージ、バックアップの作成、管理、制御、監視を自動化できます。実行されたアクティビティは AWS CloudTrail サービスにログとして記録されます。セキュリティの自動化により、電力事業者はデフォルトによる拒否の機能など、セキュリティベースの措置を自動化することで、事前

対応型のインシデント対応機能を装備でき、セキュリティイベントの範囲と影響を軽減できます。

電力事業者は AWS CloudFormation を使用して Infrastructure as Code (IaC) を実現することにより、関連する AWS リソースのコレクションをモデリングし、これらのプロビジョニングを迅速に一貫して行い、ライフサイクル全体で管理できます。ネットワーク全体、そのサブネット、ルートテーブル、セキュリティ (NACL とセキュリティグループルール)、Amazon EC2 インスタンスの記述と起動には、CloudFormation テンプレートを使用できます。さらに、AWS CloudFormation を使用すると、Amazon EC2 インスタンスへのソフトウェアのインストールと設定、VPN 接続の設定と確立、自動化を使用したほとんどの AWS のサービスの起動と設定を行うことができます。

CloudFormation スタックを定義しておくと、再実行して同一の環境を生成することもできます。これにより、テスト環境と開発環境を構築する作業が、数週間から数か月ではなく、数分から数時間で完了します。また、電力事業者のクラウドインフラストラクチャ全体の復元も、最小限の労力によってオンデマンドで復元できます。この機能は、高可用性、業務の継続性、ディザスタリカバリ (訓練時にも実際の災害発生時にも) の実現に役立ちます。

AWS が提供する自動化は、電力事業者のセキュリティとコンプライアンスプログラムを全側面からサポートします。具体的には、アイデンティティとアクセス管理 (CIP-004)、セキュリティイベントモニタリング (CIP-007)、インシデント対応 (CIP-008)、復旧 (CIP-009)、ベースラインの確立と維持 (CIP-010) の分野に対応しています。

大規模環境でのガバナンス

電力事業者は CIP-002 のシステム分類を使用して CIP への準拠を開始し、対象範囲内のシステムを特定して、どの CIP-002 定義に適合するかに応じ、リスク影響レベル

(「高」、「中」、「低」) を適用します。AWS では、複数のアカウントを使用して、目的およびリスクプロファイルが異なるシステムを分離することをお勧めしています。このアプローチは、一元的なソースからアカウントを管理しながら、責任の分離を実装/実証し、システム間で生じるリスクを制限するために役立ちます。ワークロードを実行し、アクセスのログ記録/監視/制御を行い、一般的なセキュリティを実装するための、このようなアカウントの集合は、AWS ランディングゾーンと呼ばれるものです。

電力事業者でランディングゾーンを管理するために使用できる AWS のサービスには、次のようなものがあります。

- AWS Organizations は、AWS リソースの増加やスケールに合わせて、環境を一元的に管理および統制するのに役立ちます。AWS Organizations を使用すると、新しい AWS アカウントをプログラムで作成してリソースを割り当てる、アカウントをグループ化してワークフローを整理する、アカウントやグループにポリシーを適用してガバナンスを確保する、すべてのアカウントの支払い方法を一本化して請求を簡素化するなどの処理を行うことができます。さらに AWS Organizations は、一元的な設定、セキュリティメカニズム、監査要件、組織内のアカウント間でのリソース共有を定義できるように、他の AWS サービスと統合されています。
- AWS Organizations サービスコントロールポリシー (SCP) は、組織内のアクセス許可を管理するために使用できる組織ポリシーの一種です。SCP は、組織内のすべてのアカウントで利用可能なアクセス許可を一元的に制御できます。SCP は、アカウントによるアクセスを組織のアクセス制御ガイドラインの範囲内に制限するために役立ちます。
- AWS Control Tower は、電力事業者がマルチアカウントのセキュアな AWS 環境をセットアップおよび管理するためのサービスです。 AWS Control Tower は、アイデンティティ管理、アカウントへのフェデレーションアクセス、ロギングの一元管理、クロスアカウントセキュリティ監査の確立、アカウントのプロビジョニングワークフローの

定義、ネットワーク設定でのアカウントベースラインの実装を行うブループリントを提供することでアカウント管理を簡素化します。AWS Control Tower を使用すると電力事業者は、強く推奨されるガードレールと呼ばれている高レベルの必須ルールを実装できます。これは、サービスコントロールポリシー (SCP、Service Control Policy) を使用してポリシーを確実に適用したり、AWS Config ルールを使用してポリシー違反を検出するために役立ちます。

AWS ランディングゾーンのほかにも、以下のような AWS サービスは、電力事業者がセキュリティと監査目標を大規模に達成するうえで役立ちます。

- AWS Audit Manager を使用することで、電力事業者は AWS の利用を継続的に監査して、リスクの監視や、規制および業界規格への準拠状況の評価を容易に行うことができます。AWS Audit Manager の使用によって証跡収集を自動化し、監査時に行われがちな「全員参加型」の手作業を減らすとともに、ビジネスの成長に合わせてクラウドでの監査機能を拡張できます。AWS Audit Manager を使用すると、ポリシー、手順、活動 (統制とも呼ばれる) が効果的に機能しているかどうかを簡単に評価できます。監査の際に AWS Audit Manager を使用すれば、電力事業者はステークホルダーによる統制の見直しを実施しやすくなり、手作業を大幅に減らして監査用のレポートを作成できます。
- AWS Firewall Manager は、AWS Organizations 内にあるアカウントとアプリケーション全体で一元的にファイアウォールルールを設定および管理できるようにするセキュリティ管理サービスです。新規アプリケーションが作成されると、AWS Firewall Manager はセキュリティルールの共通セットを適用することで、新規アプリケーションとリソースを簡単にこれらに準拠させることができます。AWS Firewall Manager を利用することで、電力事業者は AWS Organizations のマスターアカウントから単一のサービスとして、ファイアウォールルールの構築やセキュリティポリシーの作成を行い、それらをインフラストラクチャ全体を一貫的で階層的な管理方法で管理できます。

- AWS Systems Manager インベントリを使用すると、Amazon Elastic Compute Cloud (Amazon EC2) サーバーとオンプレミスのコンピューティング環境を可視化することで、電力事業者はクラウド内のシステムのセキュリティを管理および統制できます。電力事業者は、AWS Systems Manager インベントリを使用してマネージドインスタンスからメタデータを収集し、そのメタデータを Amazon Simple Storage Service (Amazon S3) バケットに一元的に保存することにより、組み込みツールを使用してデータを照会し、ソフトウェアポリシーによって求められるソフトウェアや設定をどのインスタンスが使用していて、どのインスタンスの更新が必要であるかをすばやく判断できます。クラウド上のリソースを管理する場合に NERC CIP 要件を満たすことができるように、AWS ではお客様が AWS リソースにタグの形式でメタデータを割り当てることができます。これにより、クラウド内の規制されたワークロードについて、BES サイバー分類を文書化することができます。

- Amazon CloudWatch は、AWS CloudTrail のログや、CloudWatch エージェントを使用してサーバーから収集されたログで、特定の条件が満たされた場合にイベントを自動的に作成するように設定できます。これらのイベントは、修復アクションと通知をトリガーするために使用できます。

- AWS Systems Manager Session Manager は、セキュアで監査可能なインスタンス管理を提供します。インバウンドのポートを開いたり、踏み台ホストを維持したり、SSH キーを管理したりする必要はありません。また、Session Manager では、インスタンスへの制御されたアクセス、厳格なセキュリティプラクティス、完全に監査可能なログ (インスタンスアクセスの詳細を含む) を必要とする企業ポリシーに簡単に準拠できます。同時に、エンドユーザーには Amazon EC2 インスタンス (仮想マシン) へのシンプルなワンクリックのアクセスを提供します。

以下の各セクションでは、AWS クラウドのサービスを使用しているお客様が、NERC CIP 標準で定められたセキュリティ目標をどのように満たしているかを示します。

ID とアクセスの管理

CIP-004 (人事とトレーニング) には、アクセスの認証、監査、取り消しに関する要件が含まれています。クラウドでこれらの要件に対処するには、クラウドの設定と管理アクティビティを実行するためのアクセス (AWS マネジメントコンソール)、クラウド内のサーバーへのリモートアクセス (Amazon EC2 インスタンスへの SSH と RDP アクセス)、アプリケーションへのエンドユーザーアクセスを管理します。AWS には、これらすべてのカテゴリのユーザーをきめ細かなレベルで管理するためのサービスが用意されています。

クラウドの設定と管理アクティビティを実行するためのアクセスは、AWS Identity and Access Management (IAM) で管理されます。IAM では、AWS サービスの API、AWS マネジメントコンソール、特定のリソースに対するアクセスの管理、承認、アクセス権限の検証、アクセス権限の取り消しを行うことができます。IAM を使用すると、電力事業者はユーザー、ロール、グループを作成し、きめ細かなアクセス許可を割り当てることができます。電力事業者は、Microsoft Active Directory など既存の SAML 2.0 互換ディレクトリサービスを使用してユーザーまたはグループを IAM ロールにマッピングすることで、IAM との統合を実現できます。電力事業者は、アクセス管理用として IAM と AWS Single Sign-On (SSO) サービス (訳注：2022 年 11 月現在で、「AWS IAM Identity Center」にサービス名が変更されています) のみの使用を選択することもできます。これらのサービスを使用すると、単一ポイントでユーザー、アクセス、廃止プロセスを管理できるため、アクセス管理が簡素化されます。例えば、パスワード設定の統制 (複雑さ、長さ、有効期限) は、IAM または IAM と統合される既存のディレクトリサービスで管理できます。

AWS の IAM Access Analyzer では、既存のアクセスを確認して、外部または未使用の意図しないアクセス許可を特定し、削除できます。また、IAM Access Analyzer は自動推論を使用し、AWS アカウントの外部からアクセスできるリソースについて、包括

的な分析結果を生成します。この分析では、IAM Access Analyzer は、新規または更新されたリソースポリシーを継続的に監視し、Amazon S3 バケット、AWS KMS キー、Amazon SQS キュー、IAM ロール、AWS Lambda 関数、AWS Secrets Manager シークレットに付与されたアクセス許可を分析します。

電力事業者のシステム管理者チームは、クラウド内で SSH または RDP を介して、Amazon EC2 インスタンスにアクセスできます。電力事業者で Amazon EC2 インスタンスに対する管理アクセスを行うには、既存のディレクトリサービスである AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD とも呼ばれます) を使用できます。さらに AWS には、SSH と RDP 用にポートを開くことなく Amazon EC2 インスタンスへの接続またはコマンド実行を行うための手段として、Session Manager が用意されています。Session Manager へのアクセス許可は、IAM を介して付与されます。Amazon EC2 インスタンスへのユーザーアクセスを設定し、IAM のアクセス許可ポリシーを通じて Session Manager へのアクセスを提供する作業は電力事業者が行います。

エンドユーザーは、AWS 上のデータに対しても、電力事業者の既存のディレクトリサービスや IAM 連携によりアクセス制御することが可能です。また、AWS 上のアプリケーションについても既存ディレクトリ、IAM アクセス制御に加えて、Amazon Cognito によるアクセス制御が可能です。Amazon Cognito は、お客様のエンドユーザーによる、ウェブおよびモバイルアプリケーションへのサインアップ、サインイン、アクセス制御をサポートしています。

データ保護

電力事業者は、保管中、転送中、使用中のデータについて、ライフサイクル全体を通じてデータを保護するための要件 (CIP011-2、情報の保護) を満たすことができます。AWS では、データ統制、データプライバシー、データ主権、データセキュリティをお客様に提供できるよう尽力しています。

電力事業者には AWS 上のデータに対する完全な統制権があり、AWS のサービスとツールを使用して、どこにデータを保存し、どのようにデータを保護して、誰にアクセスを許可するかを決定できます。AWS Identity and Access Management (IAM) などのサービスを使用すると、電力事業者は AWS のサービスとリソースへのアクセスを安全に管理できます。AWS Key Management Service (AWS KMS) と AWS CloudHSM により、電力事業者は暗号化キーを安全に生成および管理できます。AWS の従業員がお客様のキーをエクスポートまたは使用することはできません。

AWS Key Management Service (AWS KMS) は、可用性の高いフルマネージドサービスです。キー管理機能と暗号化関数は、ほとんどの AWS のサービスと統合されています。AWS KMS には単一の制御ポイントがあり、これによって、統合された AWS のサービスとお客様のアプリケーションに関して、キー管理とポリシー定義を一貫して行います。電力事業者は AWS マネジメントコンソール、AWS SDK、または CLI を使用して、キーのアクセス許可を簡単に作成、インポート、ローテーション、削除、管理できます。AWS KMS は AWS のサービスと統合されており、AWS のワークロード全体のデータを暗号化するためのキーの使用を簡素化します。電力事業者は、暗号化されたリソースをアカウントやサービス間で共有する機能を含め、必要なアクセス制御レベルを選択します。AWS KMS は、キーの使用をすべて AWS CloudTrail のログに記録し、ユーザーに代わってキーを使用した AWS のサービスを含め、暗号化されたデータに誰がアクセスしたかを独自に示します。

お客様は AWS CloudHSM を使用することもできます。これは、クラウドベースのハードウェアセキュリティモジュール (HSM) であり、AWS クラウド上で独自の暗号化キーを簡単に生成して使用できるサービスです。AWS CloudHSM では、FIPS 140-2 レベル 3 認証済みの HSM を使用して、暗号化キーを管理できます。AWS CloudHSM により、PKCS#11、Java Cryptography Extensions (JCE)、Microsoft CryptoNG (CNG) ライブラリといった業界標準の API を使用して、アプリケーションを柔軟に統合できます。HSM を信頼の基点 (root of trust) として使用する

ことは、セキュリティ、プライバシーをはじめ、HIPAA、FedRAMP、PCI といった不正使用防止規制のコンプライアンスを証明するのに役立ちます。

または、オンプレミスのキー管理と HSM ソリューションからキーをインポートすることで、キーに対するローカル統制を維持しながら、AWS KMS の機能を引き続き利用することもできます。AWS KMS の HSM ファームウェアのアップデートは、FIPS 140-2 に準拠した NIST 認定ラボと Amazon 内の独立したグループとによって監査・レビューされるマルチパーティアクセスコントロールによって制御されます。

データのプライバシーについては、電力事業者がデータを保護するために活用できるさまざまなベストプラクティスの文書やガイダンスを AWS が提供しています。AWS カスタマーアグリーメントに記述されているように、AWS がお客様の同意を得ることなくお客様のデータを使用または共有することはありません。AWS は、クラウドセキュリティに関する ISO 27017、クラウドプライバシーに関する ISO 27018 などの認証と認定を取得しています。

データ主権については、電力事業者がデータの保存先として AWS リージョンを選択します。電力事業者は、選択した AWS リージョンにデータが保持されていると確信を持ちながら AWS のサービスを使用できます。AWS は、サービスを維持または提供するために必要な場合、または法律あるいは行政機関による拘束力のある命令に従うために必要な場合を除き、お客様のコンテンツへのアクセスまたは使用を行いません。電力事業者は、コンテンツの所有権と統制権に加え、組織のセキュリティポリシーに沿ってコンテンツの暗号化、保護、移動、削除を行う権利を保持します。電力事業者が AWS のストレージサービスにデータを保存する場合 (保管中のデータ) や、AWS のネットワーク経由でデータを転送する場合 (転送中のデータ) には、暗号化の使用を強くお勧めしています。

クラウド内のセキュリティは、AWS とお客様の間で共有される責任です。電力事業者は、Amazon GuardDuty を使用する場合も、Amazon EC2 インスタンスの基盤と

なるプラットフォームである AWS Nitro System のいずれを使用する場合も、AWS の包括的なサービスを使用して、コアセキュリティ、機密性、コンプライアンスの要件への対応を強化できます。さらに、AWS CloudHSM や AWS Key Management Service などのサービスにより、電力事業者は暗号化キーを安全に生成および管理できます。AWS Config と AWS CloudTrail は、コンプライアンスと監査のための監視機能とログ記録機能を提供します。

電力事業者が使用中のデータを保護する方法は複数ありますが、1 つの選択肢は、機密性の高いワークロードの処理に AWS Nitro Enclaves を使用することです。AWS Nitro Enclaves は、最も機密性の高いデータを処理するアプリケーションにおいて、お客さまが攻撃対象領域を削減するのに役立ちます。Enclaves は、重要機密を扱うアプリケーションをホストするための、強化かつ分離され、高度な強制力を持つ環境を提供します。Nitro Enclaves には、ソフトウェア用の暗号化証明書が含まれています。これにより、認証のあるコードだけが正確に実行されるようにできます。同時に、AWS Key Management Service との統合も行え、自身の Enclaves からのみ機密情報にアクセスできるようにします。

AWS では、規格に従ってデバイスの設置、修理、および破棄 (最終的に不要になった場合) を行います。ストレージデバイスが耐用年数に達すると、AWS は NIST SP800-88 に詳細が説明されている手法で、そのメディアの運用を停止します。電力事業者のデータが保存されているメディアは、安全に運用停止が完了するまで AWS の統制対象です。電力事業者は、Amazon EBS ボリュームに暗号化 (AWS KMS) を使用してデータをさらに保護することも、ストレージメディアを再利用または廃棄する前にサードパーティ製ソフトウェアを使用してデータを完全に消去することもできます。

論理的な分離とセキュアなネットワーク

電力事業者は、Amazon Virtual Private Cloud (Amazon VPC) を使用してクラウドネットワークを定義し、インターネットへの露出を制限して、すべてのネットワークト

ラフィックを検査、保護、制御することにより、通信を制限し (CIP-005、電子的セキュリティ境界)、悪意のある通信による脅威を軽減できます。

AWS Web Application Firewall (AWS WAF) は、アプリケーションの可用性、セキュリティの侵害、リソースの過剰消費に影響を及ぼす可能性のある一般的なウェブの脆弱性から、ウェブアプリケーションを保護するために役立ちます。電力事業者では、AWS WAF を使用すると、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や、特定のアプリケーション用に設計されたルールを作成できます。

電力事業者は、一般的なネットワークの脅威からの保護を提供するサービスとして AWS Network Firewall を使用することで、AWS 上の VPC をさらに保護できます。AWS Network Firewall のステートフルファイアウォールでは、接続の追跡やプロトコルの識別などのトラフィックフローからコンテキストを取り込み、VPC が不正なプロトコルを使用してドメインにアクセスするのを防ぐなどのポリシーを適用できます。

AWS Network Firewall の侵入防止システム (IPS、Intrusion Prevention System) では、アクティブなトラフィックフロー検査により、シグネチャベースの検出を使用して脆弱性の悪用を特定してブロックします。また、AWS Network Firewall は、既知の不正な URL へのトラフィックを停止し、完全修飾ドメイン名を監視できるウェブフィルタリングも提供します。電力事業者では AWS Shield の自動保護を活用することで、ウェブサイトやアプリケーションを標的として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 攻撃に対して防御することができます。

設定、脆弱性、パッチ管理

電力事業者は AWS のサービスを使用して、設定変更管理、脆弱性管理 (CIP-010、設定変更管理と脆弱性評価)、パッチ適用と悪意のあるコードからの保護 (CIP-007、システムセキュリティ管理) に関するセキュリティ目標に取り組むことができます。

AWS では、AWS CloudFormation などのテンプレート定義や管理ツールを使用して、標準的な事前設定済みのクラウド環境を構築できます。AWS CloudFormation は、承認されたベースラインに新しいデバイスを構築する際の手動エラーを減らすために、自動テンプレートの使用をサポートしています。AWS CloudFormation を使用すると、電力事業者はサービスを通じて変更が行われたときに設定のドリフトを検出できます。これは、電力事業者で未承認のベースライン変更の特定やベースラインレビューを行う方法の 1 つです。

AWS Config を使用すると、お客様は AWS リソースの設定を望ましい設定と比較して評価、監査、評価できるため、ベースラインレビューと変更管理プロセスを簡素化できます。AWS Config ルールを使用すると、動的なコンプライアンスチェックが可能になります。これにより、クラウド設定の変更に関して検出、修正を行い、リアルタイムでイベントの通知を受け取ることができます。イベント通知も、電力事業者が未承認のベースライン変更を特定するための方法の 1 つです。

AWS には、組織の基準、ベストプラクティス、規制の要件にクラウドリソースを準拠させつつ電力事業者での対応速度を向上できるように、幅広いツールが用意されています。Amazon Inspector は、アプリケーションの脆弱性やベストプラクティスからの逸脱 (影響を受けるネットワーク、OS、接続されたストレージを含む) を自動的に評価できるセキュリティ評価サービスです。組織の基準に従って AWS リソースの作成と廃止を管理するには、デプロイツールを使用します。

多数の AWS パートナーが、悪意のあるコードから保護するサードパーティホストベースの検出ソフトウェアや、CIP-010 の脆弱性評価要件への対応に使用できる、AWS 上のサーバーをスキャンするサードパーティ製脆弱性評価ツールを提供しています。

AWS では、電力事業者はパッチ管理用にサードパーティ製ソフトウェアを使用することも、AWS Systems Manager Patch Manager を使用し、セキュリティ関連のパッチと、それ以外のタイプの更新の両方を対象として、マネージドインスタンスへのパッチ適用プロセスを自動化することもできます。

セキュリティイベントの監視活動

CIP-007 (システムセキュリティ管理) には、セキュリティイベントの監視活動に関する要件が含まれています。セキュリティイベントは、API コール、アプリケーション/サーバーログ、AWS のサービスから発生します。AWS 上のアクションはすべて、AWS API でサポートされているウェブサービスの呼び出しです。これらの API コールは、AWS CloudTrail が有効であればログに記録されます。このアプローチでは、API コールを詳細に可視化し、コールの実行者、内容、発生時点、発生場所などを特定できます。調査とコンプライアンスレポートを効率化するには、ログ集計オプションを利用できます。また、Amazon CloudWatch を通じてアラート通知を設定しておき、特定のイベントが発生した場合やしきい値を超えた場合に通知を受け取ることもできます。電力事業者ではこれらのツールや機能を使用することで、ビジネスに影響が及ぶ前に問題を検出するための可視性を得て、業務環境におけるセキュリティ体制の強化、コンプライアンスのサポート、リスクプロファイルの軽減を図ることができます。

さらに、サーバーからアプリケーションとサーバーのログを収集して Amazon CloudWatch に送信し、アラームを設定して通知を受け取ることができます。電力事業者は AWS Lambda を使用して、アラームがトリガーされた場合の修復アクションを

実装できます。このアプローチにより、電力事業者は監視活動にとどまらず、ほぼリアルタイムでイベントを検出して修復できます。

ほとんどの AWS のサービスでは、その機能特有のログも生成されます。例えば、VPC フローログを有効にすることで、電力事業者は VPC 内のトラフィックを可視化できます。イベントの監視と検出には、Amazon GuardDuty を使用できます。これは、悪意のあるアクティビティや不正な動作を継続的に監視する脅威検出サービスです。このサービスでは、機械学習、異常検出、総合的な脅威インテリジェンスを使用し、AWS CloudTrail、VPC フローログ、DNS ログなど、複数の AWS データソースに関するイベントから潜在的な脅威を特定し、優先順位を付けます。Amazon CloudWatch Events と統合することで、Amazon GuardDuty のアラートを使用して複数のアカウントにわたる集計を容易に行い、既存のイベント管理システムやワークフローシステムに簡単にプッシュできます。電力事業者は Amazon Detective を使用して、ログや Amazon GuardDuty のイベントをさらに分析して調査を進め、セキュリティ上の潜在的な問題や不審なアクティビティの根本原因をすばやく特定できます。Amazon Detective では、AWS リソースからログデータを自動的に収集し、機械学習、統計的分析、グラフ理論を使用して、より迅速かつ効率的なセキュリティ調査を簡単に行うことができます。

AWS Security Hub では、電力事業者のすべての AWS アカウントにわたり、セキュリティアラートとセキュリティ状況を包括的に確認できます。ファイアウォールやエンドポイント保護、脆弱性スキャナ、コンプライアンススキャナなど、企業が自由に使える強力なセキュリティツールがありますが、チームはこれらのツールを切り替えながら、毎日何百、時には何千ものセキュリティアラートに対処することができます。AWS Security Hub では、Amazon GuardDuty、Amazon Inspector、AWS Identity and Access Management (IAM) Access Analyzer、AWS Systems Manager、AWS Firewall Manager、AWS Firewall Manager など複数の AWS のサービスや、AWS

パートナーネットワーク (APN) ソリューションからのセキュリティアラートまたは検出結果を一元的に集計、整理、優先順位付けできます。

AWS Systems Manager の機能である Application Manager は、システム管理者がアプリケーションのコンテキストで AWS リソースに関する問題を調査および修正する際に役立ちます。Application Manager は、複数の AWS のサービスと AWS Systems Manager の機器からの運用情報を 1 つの AWS マネジメントコンソールに集約します。Application Manager で、電力事業者が運用する AWS リソースの論理グループの単位は、アプリケーションごとまたはサイバーシステムごとです。Application Manager は、すべての AWS リソースに関するメタデータをリソースグループに編成した形でインポートします。Application Manager は、AWS CloudFormation、Amazon Elastic Kubernetes Service (Amazon EKS)、AWS Launch Wizard によって作成されたリソースに関するメタデータも自動的にインポートします。このメタデータが収集されると、Amazon CloudWatch によってトリガーされるアラーム、AWS Config および AWS Systems Manager State Manager から提供されるコンプライアンス情報、Amazon EKS から提供される Kubernetes クラスター情報、AWS CloudTrail および Amazon CloudWatch Logs から提供されるログデータ、AWS Systems Manager OpsCenter から提供される情報、ホスト元の AWS のサービスから提供されるリソース詳細が、Application Manager による単一のダッシュボードに表示されます。

インシデント対応

電力事業者には、調査を管理し、潜在的なインシデントや確認済みのインシデントに対応するための系統立ったアプローチが必要です。CIP-008 (インシデントレポートと対応計画) には、インシデント対応、復旧、再構成に関する計画、報告、管理の要件が定義されています。AWS のインシデント対応のプラクティス、ポリシー、プログラム (インシデント対応テストを含む) は、保証プログラムの一環として、独立したサードパーティ評価機関によって評価されます。

AWS では、インシデント対応戦略の実装や、イベントの監視と調査を可能にするさまざまなツールやサービスもお客様に提供しています。『AWS セキュリティインシデント対応ガイド』には、お客様がセキュリティ規格に準拠するために使用できる詳細情報と戦略が記載されています。

レジリエンスとシステム復旧

レジリエンスと可用性は電力網の信頼性にとって最優先であり、その裏付けとして AWS クラウドのインフラストラクチャでは、有益なリソースを提供しています。AWS のインフラストラクチャは、停止やインシデントを最小限に抑えるように設計されています。また、中断が発生した場合はお客様への影響を抑え、サービスの継続性を維持するように構築されています。

AWS は、複数の地理的リージョン内にデータセンターを構築しています。各リージョンは、複数のアベイラビリティーゾーン (AZ) で構成されています。現在、北米内には、2 つの GovCloud リージョンと 25 の AZ を含む 7 つの AWS リージョンがあります。これらの AZ によってお客様は、単一のデータセンターの場合より高い可用性、耐障害性、拡張性で本稼働用アプリケーションとデータベースを運用できるだけでなく、システムの中断に対する最大限のレジリエンスも実現できます。AWS リージョンとアベイラビリティーゾーンの最新情報については、「AWS グローバルインフラストラクチャ」を参照してください。

どのような組織についても、可用性とレジリエンスの目標を達成するには、復旧計画の文書化とテストが不可欠です。CIP-009 (*BES* サイバーシステムの復旧計画) には、復旧計画、バックアップ、テストの要件が定義されています。お客様は、AWS Backup や AWS Elastic Disaster Recovery などの AWS のサービスを使用して、可用性とレジリエンスに優れたアプリケーションを構築してデプロイできます。目標復旧時間 (RTO) に基づき、電力事業者は単一の AWS リージョンで複数のアベイラビリティーゾーンにまたがってシステムをデプロイするか、瞬時または瞬時に近いフェイルオー

バーで複数の AWS リージョンにまたがってデプロイするかを選択できます。電力事業者は、自動でアプリケーションをデプロイする AWS のベストプラクティスを使用して、ディザスタリカバリのプロセスを高速かつ低コストでテストできます。

リモート、エッジ、オンプレミスコンピューティング

電力事業者は、BES サイバーシステムを送電設備と共に、データセンター、発電施設、変電所、コントロールセンターに分散させることができます。すべてのロケーションでテクノロジーの整合性を維持し、すべてのシステム間でゼロトラストのセキュアな通信を確保することは、BES の運用において非常に重要になります。AWS は、分散コンピューティングとデータ取得の要件を安全に満たすために電力事業者が使用できるさまざまな製品とサービスを提供しています。AWS Outposts は、AWS インフラストラクチャ、AWS のサービス、API、ツールを変えることなく、事実上すべてのデータセンター、コロケーションスペース、オンプレミス施設において、真に一貫性のあるハイブリッド環境を実現するフルマネージドサービスです。AWS Outposts は、ローカルシステムで相互依存性のあるアプリケーションの移行、データレジデンシー、ローカルのデータ処理、オンプレミスシステムに低レイテンシーでアクセスする必要があるワークロードに最適です。AWS のコンピューティング、ストレージ、データベース、およびその他のサービスは AWS Outposts でローカルに実行されます。電力事業者は、そのリージョンで利用可能な AWS のあらゆるサービスにアクセスし、使い慣れた AWS のサービスとツールを用いてオンプレミスアプリケーションを構築、管理、スケーリングすることができます。

AWS Snowball Edge Compute Optimized デバイスは、分離された環境における高度な機械学習やフルモーションビデオ分析などのユースケースのために、52 個の仮想中央処理ユニット (vCPU、Virtual Central Processing Unit)、ブロックストレージとオブジェクトストレージ、オプションのグラフィック処理ユニット (GPU、Graphics Processing Unit) を提供します。電力事業者はこれらのデバイスを、接続が断続的な

環境や極度の遠隔地でのデータ収集、機械学習と処理、ストレージに使用できます。また、これらのデバイスをラックマウント型でクラスター化し、大型の設備を構築することもできます。AWS Snowball は、特定の Amazon EC2 インスタンスタイプと AWS Lambda 関数に対応しているため、電力事業者は AWS クラウドでアプリケーションを開発してテストし、その後遠隔地のデバイスにデプロイすることで、データを収集して処理することができます。

AWS IoT は、暗号化やデバイスデータへのアクセス制御などの予防的なセキュリティメカニズムや、設定を継続的に監視し監査するサービスなど、あらゆるセキュリティレイヤーに対応するサービスを提供しながら、産業用ソリューション向けのサービスを提供します。デバイスへの接続は x.509 証明書を使用して保護され、AWS IoT Device Defender のようなサービスで、インダストリアル IoT デバイスのフリートを保護できます。AWS IoT Device Defender は、IoT の設定を継続的に監査して、セキュリティのベストプラクティスから逸脱していないことを確認し、侵害の兆候が疑われる異常なデバイスの動作を継続的に監視して検出します。AWS IoT Device Management を使用すると、膨大な数の IoT デバイスの登録、編成、モニタリング、リモート管理を簡単かつ安全に行うことができるようになります。AWS IoT セキュアトンネリングを使用すると、リモートサイトの制限付きファイアウォールの内側にあるインダストリアル IoT デバイスに安全に接続して、トラブルシューティング、設定の更新、その他の運用タスクを実行できます。AWS IoT Jobs は、AWS IoT に接続された 1 つ以上の IIoT デバイスに送信および実行される一連のリモート操作 (ソフトウェアやファームウェアの更新など) を定義するために使用できます。

AWS Certificate Manager (ACM) は、クラウドで X.509 証明書を生成して署名できる AWS のマネージドサービスです。ACM の柔軟性により、電力事業者は独自の CA を使用し、AWS で証明書署名の操作を実行できます。AWS は、CA が ACM サービス上で保持されている物理インフラストラクチャを保護します。電力事業者は、自

分のアカウントで ACM サービスにアクセスできるユーザーに対し、適切なポリシーを定める責任を負います。

物理的セキュリティ

CIP-006 (BES サイバーシステムの物理的セキュリティ) は、各責任主体に対し、物理的アクセス制御、(許可済みおよび無許可の) アクセスのログ記録/監視などのセキュリティ対策を織り込み、文書化された物理的セキュリティ計画を実施するよう求めています。電力事業者は、クラウドインフラストラクチャを物理的に保護する AWS データセンターの統制を継承できます。この統制は、境界、建物への進入口、データセンターの各フロアへのアクセスを厳密に管理するものです。AWS は、人為的リスクおよび自然災害によるリスクからデータセンターを保護するために、データセンターの設計とシステムに関する革新を続けています。AWS のデータセンターは、それぞれアクセス制御とセキュリティを実装したレイヤーで構成されており、セキュリティとコンプライアンスの確認のためにサードパーティによる監査を受けています。

AWS データセンターの物理的なセキュリティは、**境界防御レイヤー**から始まります。このレイヤーには、警備員、フェンス、セキュリティフィード、侵入検知テクノロジー、その他のセキュリティ対策など、場所に応じた多数のセキュリティ機能が含まれています。AWS は、業務上の正当な理由で立ち入る必要がある人々に限定して物理的なアクセスを許可しています。データセンターへの入場を必要とする従業員とベンダーは、まずアクセスを申請し、業務上の正当性を詳しく説明する必要があります。アクセスが許可された場合、必要な業務が完了した時点で、このアクセスは失効します。立ち入りを許可された人はバッジを渡されます。このバッジにより、多要素認証が実行され、アクセスが事前に承認されたエリアに制限されます。データセンターに日常的に出入りする AWS の従業員は、職務に基づいて施設の関連エリアへのアクセスを許可されます。エリアアクセスマネージャーはスタッフリストを定期的に見直し、従業員ごとに許可が引き続き必要かどうかを確認します。

インフラストラクチャレイヤーは、データセンターの建物と、データセンターの稼働に必要な設備とシステムで構成されています。バックアップ電源装置、HVAC システム、消火装置などのコンポーネントはすべて、インフラストラクチャレイヤーの一部です。これらのデバイスとシステムは、サーバーの保護を支えており、結果的にお客様のデータの保護にも役立っています。AWS では、インフラストラクチャの各レイヤーに対して、厳格なアクセス制御を実装しています。インフラストラクチャレイヤーへのアクセスは、ビジネスニーズに基づいて制限されます。レイヤーごとのアクセス確認が実装され、デフォルトでは各レイヤーに立ち入る権限が付与されません。特定のレイヤーにアクセスする具体的な必要性がある場合のみ、そのレイヤーへのアクセスが許可されます。水道、電気、通信、インターネット接続は、緊急時にも運用を継続できるように、冗長性を持つように設計されています。電気系統は完全な冗長設計になっているため、停電の際は無停電電源装置から特定の機能に電力が供給され、発電機から施設全体に非常用電力が供給されます。人による監視とシステムによる監視で温度と湿度を制御することで、過熱を防止し、サービス停止の発生を抑制できます。

データレイヤーは、AWS データセンター内でお客様のデータを保持する唯一の領域であり、最も重要な保護ポイントです。防御策はアクセスを制限し各レイヤーにおいて特権を分離することから始まります。さらに AWS では、このデータレイヤーをさらに保護するために、脅威検出機器、監視カメラ、システム的な手続きを備えています。データレイヤーに立ち入るための許可を取得するには、必須の手順があります。これには、権限を持つ担当者による、アクセス申請の確認と承認が含まれます。この間に、脅威検知システムと電子的な侵入検知システムで監視し、脅威や不審な行動が確認された場合は、自動的にアラートをトリガーします。

サーバールームへのアクセスポイントは、多要素認証を義務付ける電子制御デバイスで厳重に保護されています。技術的な侵入を防ぐため、AWS のサーバーはデータ削除を試みる従業員に警告することができます。万一、違反が発生した場合には、サーバーが自動的に無効化されます。お客様のデータの保存に使用されるメディアストレージデバ

イスは、AWS の分類で「クリティカル」であり、そのライフサイクルを通じて影響レベルの高い要素として適切に取り扱われます。ストレージデバイスが耐用年数に達すると、AWS は NIST SP800-88 に詳細が説明されている手法で、そのメディアの運用を停止します。お客様のデータが保存されているメディアは、安全に運用停止が完了するまで AWS の統制対象です。

環境レイヤーは、立地の選択、建設、運用/維持に至るまで、環境に固有の要因について考慮されています。AWS では、洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。

クラウドサービスの使用計画に関する考慮事項

クラウド導入に向けた取り組み方は、組織ごとに異なります。クラウドへの移行を成功させるには、組織の現在の状態や、求められる目標のほか、その目標を達成するためにどのような移行が必要になるかを理解することが重要です。目標を設定する場合、電力事業者はリスクベースのアプローチを使用して、AWS に内部セキュリティ要件を実装する必要があります。

開発プロセスでは、コンプライアンスによる信頼を得るために、NERC または地域の電力事業者の監査人との協力が重要になることがあります。対話を開始し、透明性を確保して、監査人の視点や期待を理解することは、目標を設定し、作業の流れを構築するうえで役立ちます。これによってスタッフがクラウドでスムーズに業務を行えるだけでなく、コンプライアンスの実証に必要な証拠の必要性が明確になります。

電力事業者は、クラウドサービスの実装向けに用意されているリソースを使用できます。該当するリソースは、「電力事業者向けのリソース」セクションで紹介され、「その他のリソース」セクションに掲載されています。AWS では、クラウド導入の過程で電力事業者をサポートできるよう、要員向けリソース、Immersion Day、Game

Day などをご用意しています。詳しくは、AWS アカウントマネージャーまたは AWS 日本担当チームまでお問い合わせください。

寄稿者

本書の寄稿者は次のとおりです。

- Ranjan Banerji (Principal Partner Solutions Architect, Power & Utilities, AWS)
- Maggy Powell (Principal Industry Specialist, Power & Utilities, AWS Security)
- Kristine Martz (Industry Specialist, Power & Utilities, AWS Security)

その他のリソース

詳細については、次を参照してください。

- NIST サイバーセキュリティフレームワーク
- IDC Technology Spotlight – クラウド導入で電力とエネルギー業界の企業により大きな価値をもたらす
- AWS クラウド導入フレームワーク
- AWS クラウド導入フレームワーク: セキュリティのパースペクティブ
- AWS Well-Architected フレームワーク
- AWS Well-Architected フレームワーク: セキュリティの柱
- AWS Well-Architected フレームワーク: IoT レンズ
- データセンターの統制

- AWS セキュリティのベストプラクティス
- インダストリアル IoT ソリューションにおける 10 のセキュリティゴールデンルール
- AWS インシデント対応
- コンプライアンスに関するよくある質問への AWS の回答
- AWS での論理的分離
- AWS Foundational Security Best Practice コントロール
- Control Tower のベストプラクティス
- 複数 VPC のネットワーキング
- 電力とエネルギー: 本稼働までの工程 (情報ガイド)
- AWS クラウドセキュリティのためのエグゼクティブガイド
- AWS セキュリティ制御ドメインのためのエグゼクティブガイド

ドキュメントの改訂

日付	説明
2020 年 1 月	初版発行
2021 年 11 月	AWS のセキュリティおよびコンプライアンスサービスに関する内容を追加し、NERC CIP 標準の改訂に合わせて内容を更新しました。

付録: AWS のサービスと NERC CIP への適合

次の表は、AWS のサービスおよび統制の継承を使用して、NERC CIP への準拠を実証する方法と、クラウド「**内**」のセキュリティに関するお客様向け考慮事項の概要を示しています。AWS の責任である CIP 標準および要件に対応して実装された統制の詳細については、前述のセキュリティ保証レポートを参照してください。

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
CIP-002-5.1a, R1	サイバーシステムの特定と分類	AWS Tags AWS Organizations AWS Systems Manager インベントリ	電力事業者は、引き続き既存のコンプライアンスプログラムに従ってサイバーシステムを特定し、分類することができます。 システムが分類されると、電力事業者はタグ形式でメタデータを AWS リソースに割り当てて、クラウド内の規制対象のワークロードの BES サイバー分類を文書化できます。タグを使用すると、分類プロセスを強化し、定期的なシステム分類レビューの自動化をサポートできます。 各タグは、顧客が定義したキーと任意の値から成るシンプルなラベルで、リソースの管理、検索、フィルタリングを容易にします。タグを使用すると、ユーザーはリソースを目的、所有者、環境、または BES サイバーシステムの分類などの他の基準によって分類できます。	
CIP-002-5.1a, R2	15 か月ごとの確認と承認	AWS Tags AWS Organizations AWS Systems Manager インベントリ		

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
			AWS Systems Manager インベントリは、Amazon EC2 とオンプレミスのコンピューティング環境を可視化します。インベントリを使用して、マネージドインスタンスからメタデータを収集できます。このメタデータは、メインの Amazon S3 バケットに保存し、組み込みツールを使用してクエリを実行することで、どのインスタンスがソフトウェアポリシーで要求されるソフトウェアと設定を実行しているか、および、どのインスタンスを更新する必要があるかをすばやく判断できます。ワンクリック操作で、すべてのマネージドインスタンスにインベントリを設定できます。	
CIP-003-8, R1	サイバーポリシー		電力事業者は、セキュリティ管理統制に関する既存のコンプライアンスプログラムに引き続き従うことができます。お客様のサイバーポリシーとセキュリティプランを見直して、クラウドサービスの使用に対応するために必要な更新を特定する必要があります。	AWS はクラウドインフラストラクチャのセキュリティに責任を負い、クラウドインフラストラクチャのセキュリティに対処するセキュリティポリシーを維持する責任も共有しています。AWS のセキュリティポリシーは、AWS の従業員向けのセキュリティ意識向上トレーニング、物理的および論理的なアクセス制御手順、インシデント対応手順などの統制を対象としています。お客様は、
CIP-003-8, R2	影響の少ないシステムのセキュリティ計画			
CIP-003-8, R3	ドキュメント CIP シニアマネージャー			

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
CIP-003-8, R4	CIP シニアマネージャーの委任			AWS マネジメントコンソールのアーティファクトセクションで、AWS の統制を示す保証レポートを参照できます。
CIP-003-8 アタッチメント 1, セクション 1	影響の少ない BCS - サイバーセキュリティ意識		電力事業者は、セキュリティ意識向上と訓練、人員のセキュリティ、アクセス管理制御要件に関する既存のコンプライアンスプログラムを引き続き従うことができます。	AWS はクラウドインフラストラクチャのセキュリティに責任を負い、セキュリティのトレーニングと認識、人員のセキュリティ、アクセス管理と認証のための統制に対処する複数の統制フレームワークへの準拠を実証しています。AWS のお客様はこれらの統制を引き継ぎ、AWS マネジメントコンソールのアーティファクトセクションで統制の有効性を示す保証レポートを参照できます。
CIP-003-8 アタッチメント 1, セクション 2	影響の少ない BCS - 物理的セキュリティコントロール			AWS はクラウドインフラストラクチャのセキュリティに責任を負い、物理的なセキュリティの統制に対処する複数の統制フレームワークへの準拠を実証しています。AWS のお客様はこれらの統制を引き継ぎ、AWS マネジメントコンソールのアーティファクトセクションで統制の有効性を示す保証レポートを参照できます。 IT インフラストラクチャコンポーネントを収容するすべての AWS データセンターへの物理的なアクセスは、業務を実行するためにアクセスを必

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
				要とする認定済みのデータセンター従業員、ベンダー、請負業者に制限されます。施設への立ち入りは、統制されたアクセスポイントのみで許可されます。そこでは、テールゲーティングを防止し、承認された人物のみに AWS データセンターへの入館を許可するために設計された、多要素認証が求められます。AWS データセンターへのアクセス権を持つ要員のアクセスリストと認証情報は、各データセンターの Area Access Manager (AAM) が四半期ごとに確認します。
CIP-003-8 アタッチメント 1, セクション 3	影響の少ない BCS - 電子アクセス制御	AWS Identity & Access Management (IAM) IAM Access Analyzer AWS マネージドの Directory Service Amazon Cognito AWS VPN	電力事業者は、AWS IAM を使用して AWS マネジメントコンソールへの管理アクセスのユーザーアクセス、認証、取り消しを管理できます。AWS IAM では、ユーザーとロールにきめ細かなアクセス許可を実装できます。AWS IAM は、お客様の現在の SAML 2.0 互換ディレクトリサービスと統合されます。サーバー (SSH と RDP) へのアクセスとサービスへのエンドユーザーアクセスを管理するために、お客様は既存のディレクトリサービス、AWS Directory Service、AWS IAM、Amazon Cognito を使用できます。電力事業者は、これ	AWS の本稼働環境へのリモートアクセスは、定義されたセキュリティグループに限定されます。グループへのメンバーの追加は、ユーザーが環境にアクセスする必要があることを確認した権限のある個人によって確認および認証される必要があります。リモートアクセスでは、認証用に承認された暗号化チャネルを介した多要素認証が必要です。 AWS では、リモートアクセス方法の監視活動と制御を容易にする自動メカニズムを採用していま

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
		AWS Direct Connect	らのツールを組み合わせて使用することで、ユーザーの監査、ユーザーへのアクセスの許可と取り消しを行うことができます。 IAM Access Analyzer を使用すると、誰またはどのシステムが AWS アセットにアクセスできるかをより深く知ることができます。IAM Access Analyzer は継続的に稼働し、システムへの外部アクセスがあれば直ちに電力事業者の責任者に通知します。 安全なリモートアクセス管理をサポートするために、電力事業者は AWS 上のサーバーへの暗号化されたリモートアクセス用に AWS VPN を設定できます。パフォーマンスと信頼性を高めるには、AWS Direct Connect 経由で VPN 接続を確立できます。 AWS の MFA を使用して AWS 環境を保護するように多要素認証を設定できます。AWS 上のアセットへのリモートアクセス用の MFA は、既存の ID プロバイダーの機能を使用して VPN 経由で	す。監査はシステムとデバイスで行われ、レビューとインシデント調査のために独自のツールに集約されて保存されます。ネットワークやセキュリティ設定を含む AWS の運用環境は機密情報と見なされ、Amazon のデータ分類ポリシーに従って従業員によって保護される必要があります。リモート管理アクセスの試みはすべて記録され、特定の回数に制限されます。監査ログは、AWS セキュリティチームによって不正な試みや疑わしいアクティビティがないか確認されます。疑わしいアクティビティが検知されたら、インシデント対応手順が開始されます。

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
			Aamazon VPC に実装できます。また、お客様は AWS Managed Microsoft AD を使用してユーザー管理と MFA を実装することもできます。	
CIP-003-8 アタッチメント 1, セクション 4	影響の少ない BCS - サイバーセキュリティのインシデント対応	AWS CloudFormation Amazon S3 AWS CloudTrail Amazon CloudWatch Amazon OpenSearch Service	インシデント対応のプランとテストをサポートするために、お客様は AWS CloudFormation を使用してシステムのデプロイを自動化し、インシデント対応手順を迅速かつ低コストで、運用上のリスクをより低く、より頻繁にテストできる複製環境を作成する必要があります。 調査ツールとして、お客様は Amazon S3 上にデータレイクを作成して、AWS CloudTrail、他の AWS サービス、Amazon CloudWatch、システムおよびアプリケーションログからのログを保存できます。その後、お客様は Amazon OpenSearch Service を使用してイベントログを分析し、インシデント調査活動に役立てることができます。	AWS はクラウドインフラストラクチャのセキュリティに責任を負い、クラウドインフラストラクチャのインシデント対応の統制に対処する複数の統制フレームワークへの準拠を実証しています。AWS のお客様はこれらの統制を引き継ぎ、AWS マネジメントコンソールのアーティファクトセクションで統制の有効性を示す保証レポートを参照できます。 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. アクティベーションと通知フェーズ 2. 復旧フェーズ 3. 再構成フェーズ

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
				AWS のインシデント管理プランの有効性を確保するために、AWS はインシデントレスポンステストを実施しています。このテストにより、これまで知られていなかった欠陥や故障モードの発見を十分にカバーできます。さらに、Amazon のセキュリティチームとサービスチームは、潜在的なお客様への影響がないかシステムをテストし、検出と分析、封じ込め、根絶、復旧、インシデント後のアクティビティなどのインシデントに対処するためのスタッフをさらに準備できます。インシデント対応テストプランは、インシデント対応プランと併せて毎年実施されます。AWS のインシデント管理のプラン、テスト、およびテスト結果は、第三者の監査人が確認します。
CIP-003-8 アタッチメント 1, セクション 5	影響の少ない BCS - 一時的なサイバーシステムとリムーバブルメディアの悪意のあるコードのリスク軽減		電力事業者は TCA (Transient Cyber Assets) の使用に関するコンプライアンスプログラムを引き続き従うことができます。	AWS はクラウドのセキュリティに責任を負い、FedRAMP を含むいくつかの規制コンプライアンス要件を満たしています。AWS では、インフラストラクチャを保護するために FedRAMP/NIST AC-17 から 20 を含むセキュリティコントロールを実装しています。

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
CIP-004-6, R1	セキュリティ意識向上プログラム		電力事業者は、セキュリティ意識向上と訓練、人員セキュリティ、アクセス管理制御要件に関する既存のコンプライアンスプログラムを引き続き従うことができます。	AWS はクラウドインフラストラクチャのセキュリティに責任を負い、セキュリティのトレーニングと認識、人員のセキュリティ、アクセス管理と認証のための統制に対処する複数の統制フレームワークへの準拠を実証しています。AWS のお客様はこれらの統制を引き継ぎ、AWS マネジメントコンソールのアーティファクトセクションで統制の有効性を示す保証レポートを参照できます。
CIP-004-6, R2	アクセス前および 15 か月ごとのセキュリティトレーニング			
CIP-004-6, R3	人事リスク評価とバックグラウンドチェック			
CIP-004-6, R4	アクセス管理、認証、アクセス権限の検証	AWS Identity & Access Management (IAM) IAM Access Analyzer AWS マネージドの Directory Service Amazon Cognito	お客様は、AWS IAM を使用して AWS マネジメントコンソールへの管理者アクセスのユーザーアクセス、認証、取り消しを管理できます。AWS IAM では、ユーザーとロールにきめ細かなアクセス許可を実装できます。AWS IAM は、お客様の現在の SAML 2.0 互換ディレクトリサービスと統合されます。サーバー (SSH と RDP) へのアクセスとサービスへのエンドユーザーアクセスを管理するために、お客様は既存のディレクトリサービス、AWS Directory Service、AWS IAM、Amazon	
CIP-004-6, R5	ユーザーアクセスの失効			

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
			Cognito を使用できます。お客様は、これらのツールを組み合わせて使用することで、ユーザーの監査、ユーザーへのアクセス許可と取り消しを行うことができます。 IAM Access Analyzer を使用すると、誰またはどのシステムが AWS アセットにアクセスできるかをより深く知ることができます。IAM Access Analyzer は継続的に稼働し、システムへの外部アクセスがあれば直ちに電力事業者の責任者に通知します。	
CIP-005-6, R1	電子セキュリティ境界を定義し、トラフィックを外部アクセスポイントで管理し、悪意のある通信を検知	Amazon CloudFront AWS Shield Amazon Route 53 Amazon Guard Duty AWS IoT Device Defender	電力事業者は、電子セキュリティ境界管理に関する既存のコンプライアンスプログラムに引き続き従うことができます。電力事業者は、コンテンツに対する所有権と管理を維持し、電子セキュリティ境界の管理を含むセキュリティ要件を管理する責任を負います。クラウドの電子セキュリティ境界管理要件を満たすために、電力事業者は Amazon Virtual Private Cloud (VPC) を使用してクラウドネットワークの定義、インターネットへの露出の制限、設定の自動化、すべてのトラフィック (インバウンド、アウトバウンド、ネットワーク内) の検査、保	AWS はクラウドインフラストラクチャのセキュリティに責任を負い、ネットワークセキュリティとリモートアクセス管理の統制に対処する複数の統制フレームワークへの準拠を実証しています。AWS のお客様はこれらの統制を引き継ぎ、AWS マネジメントコンソールのアーティファクトセクションで統制の有効性を示す保証レポートを参照できます。 ファイアウォールや他の境界デバイスを含むネットワークデバイスは、ネットワークの外部境

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
			護、制御を行うことができます。 電力事業者は、AWS Shield を Amazon CloudFront や Amazon Route 53 とともに使用して、インフラストラクチャ (レイヤー 3 および 4) を標的とするすべての既知の攻撃を総合的に保護できます。悪意のある通信の検出をサポートするために、電力事業者は悪意のあるアクティビティや不正な動作を継続的に監視して AWS アカウントとワークロードを保護する脅威検出サービスである Amazon GuardDuty を使用できます。 AWS IoT Core または AWS IoT Greengrass を実行するリモートデバイスやエッジデバイス、ゲートウェイを保護するには、電力事業者がデバイスからの価値の高いセキュリティメトリクスを継続的に監視することで、侵害の兆候となる可能性のある異常なデバイス動作を検出 AWS IoT Device Defender を使用する必要があります。	界と、ネットワーク内の主要な内部境界のコミュニケーションをモニターし、コントロールするために配置されています。これらの境界デバイスは、ルールセット、アクセスコントロールリスト (ACL) および設定を用いて、情報の流れを、特定の情報システムサービスに向けます。ACL、またはトラフィックフローポリシーは、マネージドインターフェイスごとに確立されており、トラフィックのフローを管理し、特定の方向に送ります。ACL のポリシーは、Amazon Information Security によって承認されています。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。
CIP-005-6, R2	中間システムによるリモートアクセス管理、暗	AWS VPN AWS Direct Connect	安全なリモートアクセス管理をサポートするために、電力事業者は AWS 上のサーバーへの暗号化されたリモートアクセス用に AWS VPN を設定で	AWS の本稼働環境へのリモートアクセスは、定義されたセキュリティグループに限定されます。グループへのメンバーの追加は、ユーザーが環

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
	号化と多要素認証の活用	AWS Managed Microsoft AD AWS IoT セキュアトンネリング	きます。パフォーマンスと信頼性を高めるには、AWS Direct Connect 経由で VPN 接続を確立できます。AWS IoT セキュアトンネリングにより、電力事業者はリモートサイトの制限されたファイアウォール内で AWS IoT または AWS IoT Greengrass デバイスと双方向通信を確立できます。 AWS の MFA を使用して AWS 環境を保護するように多要素認証を設定できます。AWS 上のアセットへのリモートアクセス用の MFA は、既存の ID プロバイダーの機能を使用して VPN 経由で Amazon VPC に実装できます。また、お客様は AWS Managed Microsoft AD を使用してユーザー管理と MFA を実装することもできます。	境にアクセスする必要があることを確認した権限のある個人によって確認および認証される必要があります。リモートアクセスでは、認証用に承認された暗号化チャネルを介した多要素認証が必要です。 AWS では、リモートアクセス方法の監視活動と制御を容易にする自動メカニズムを採用しています。監査はシステムとデバイスで行われ、レビューとインシデント調査のために独自のツールに集約されて保存されます。ネットワークやセキュリティ設定を含む AWS の運用環境は機密情報と見なされ、Amazon のデータ分類ポリシーに従って従業員によって保護される必要があります。リモート管理アクセスの試みはすべて記録され、特定の回数に制限されます。監査ログは、AWS セキュリティチームによって不正な試みや疑わしいアクティビティがないか確認されます。疑わしいアクティビティが検知されたら、インシデント対応手順が開始されます。

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
CIP-006-6, R1	物理的セキュリティ計画とアクセス管理		電力事業者は、BES サイバーシステムの物理的セキュリティに関する既存のコンプライアンスプログラムに引き続き従うことができます。お客様のサイバーポリシーとセキュリティプランを見直して、クラウドサービスの使用に対応するために必要な更新を特定する必要があります。	AWS はクラウドインフラストラクチャのセキュリティに責任を負い、物理的なセキュリティの統制に対処する複数の統制フレームワークへの準拠を実証しています。AWS のお客様はこれらの統制を引き継ぎ、AWS マネジメントコンソールのアーティファクトセクションで統制の有効性を示す保証レポートを参照できます。 IT インフラストラクチャコンポーネントを収容するすべての AWS データセンターへの物理的なアクセスは、業務を実行するためにアクセスを必要とする認定済みのデータセンター従業員、ベンダー、請負業者に制限されます。施設への立ち入りは、統制されたアクセスポイントのみで許可されます。そこでは、テールゲーティングを防止し、承認された人物のみに AWS データセンターへの入館を許可するために設計された、多要素認証が求められます。AWS データセンターへのアクセス権を持つ要員のアクセスリストと認証情報は、各データセンターの Area Access Manager (AAM) が四半期ごとに確認します。
CIP-006-6, R2	訪問者管理プログラム			
CIP-006-6, R3	物理アクセス制御システムのメンテナンスとテスト			

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
CIP-007-6, R1	ポートとサービスのアクセス制限	Amazon VPC AWS Network Firewall AWS Firewall Manager	電力事業者は、システムセキュリティ管理統制に関する既存のコンプライアンスプログラムに引き続き従うことができます。電力事業者は、クラウド内のコンテンツとシステムの所有権と制御を維持し、ポートとサービスの制限、パッチ管理、悪意のあるコードの防止、セキュリティイベントの監視、システムアクセス制御などのセキュリティ要件の管理に責任を負います。 ポートとサービスのアクセスを管理するために、電力事業者はセキュリティグループとネットワーク ACL を使用して特定のポートと送信元/送信先 CIDR へのトラフィックを制限するように Amazon VPC を設定できます。Amazon S3 のアクセスポイントを使用して、Amazon S3 のデータおよびデータレイクへのアクセスを特定の VPC に制限できます。さまざまな権限セットを付与して、アクセスを微調整できます。Amazon S3 のアクセスポイントを使用すると、Amazon S3 のデータが電力事業者の VPC から離れることはありません。 AWS Network Firewall は、すべての Amazon	AWS はクラウドインフラストラクチャのセキュリティに責任を負い、システムの統制とクラウドインフラストラクチャのネットワークセキュリティに対処する複数の統制フレームワークへの準拠を実証しています。AWS のお客様はこれらの統制を引き継ぎ、AWS マネジメントコンソールのアーティファクトセクションで統制の有効性を示す保証レポートを参照できます。

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
			Virtual Private Cloud (VPC) にネットワーク保護を簡単にデプロイできるようにするマネージドサービスです。AWS Network Firewall の柔軟なルールエンジンを提供し、アウトバウンドサーバーメッセージブロック (SMB) リクエストをブロックして悪意のあるアクティビティの拡散を防ぐなど、ネットワークトラフィックを詳細に制御できるファイアウォールルールを定義できます。AWS Firewall Manager は、メインの管理者アカウントから、ファイアウォールルールを構築し、セキュリティポリシーを作成して、インフラストラクチャ全体にわたって一貫した階層的な方法でそれらを適用する単一のサービスを提供します。	
CIP-007-6, R2	パッチ管理	AWS Systems Manager AWS IoT Jobs	パッチ管理をサポートするには、電力事業者は AWS Systems Manager を使用して、パッチ、設定、カスタムポリシーに照らしてインスタンスをスキャンすることにより、セキュリティとコンプライアンスの維持を支援する必要があります。電力事業者は、パッチのベースラインの定義、アンチウイルス定義の更新、ファイアウォールポリシーの適用が可能です。また、電力事業者は大規模なサーバー群でも、各サーバーに手動でログインすることな	

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
			く、リモートで管理できます。 AWS IoT または AWS IoT Greengrass デバイスの場合、電力事業者は AWS IoT Jobs を使用してソフトウェアとファームウェアを現場のデバイスにプッシュ配信し、セキュリティの脆弱性にパッチを適用してデバイスの機能を向上させることができます。	
CIP-007-6, R3	悪質なコードの防止	Amazon GuardDuty AWS WAF	悪意のあるコードの防止をサポートするために、電力事業者は、悪意のあるアクティビティや不正な動作を継続的に監視してお客様の AWS アカウントとワークロードを保護する脅威検出サービスである Amazon GuardDuty を使用できます。電力事業者は、アプリケーションの可用性低下、セキュリティの侵害、リソースの過剰消費などの一般的なウェブの脆弱性からウェブアプリケーションを保護するウェブアプリケーションファイアウォールである AWS WAF を使用します。AWS WAF を使用すれば、電力事業者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したうえで、ウェブアプリケーションで許可またはブロックすべきトラフィックを制御できます。電力事業者は AWS WAF を使	

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
			用して、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と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できます。さらに、さまざまなサードパーティ製の IDS/IPS が AWS パートナーから入手できます。	
CIP-007-6, R4	セキュリティイベントの監視活動	AWS CloudTrail Amazon CloudWatch Amazon CloudWatch エージェント Amazon Detective Amazon S3 Amazon OpenSearch Service AWS Security Hub AWS IoT Device Defender	セキュリティイベントの監視活動をサポートするために、電力事業者は AWS CloudTrail を使用してすべての AWS API アクションのログを生成できます。さらに、電力事業者は EC2 インスタンスに Amazon CloudWatch エージェントをインストールして、アプリケーションとサーバーのログを収集できます。AWS CloudTrail と Amazon CloudWatch エージェントから生成されたログは、Amazon CloudWatch を使用して監視できます。電力事業者は、これらのログに基づいてイベントを作成し、ほぼリアルタイムでアラートを受け取ることができます。また、Amazon S3 上にデータレイクを作成してこれらのログを保存し、Amazon OpenSearch Service を使用してログの分析と監視を行うこともできます。電力事業者は、EC2 インスタンスでサードパーティ製品を使用し	

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
			てログを収集および監視できます。Amazon Detective を使用して AWS サービスからログを収集し、イベントが発生したときにセキュリティイベントの優先順位付けと調査を行うことができます。 AWS Security Hub により、電力事業者は AWS アカウント全体にわたるセキュリティアラートとセキュリティ体制を包括的に確認できます。AWS Security Hub では、Amazon GuardDuty、Amazon Inspector、AWS Identity and Access Management (IAM) Access Analyzer、AWS Systems Manager、AWS Firewall Manager など複数の AWS サービスや、AWS パートナーネットワーク (APN) のソリューションからのセキュリティアラートまたは検出結果を一元的に集計、整理、優先順位付けできます。 AWS IoT Device Defender を使用すると、電力事業者は AWS IoT または AWS IoT Greengrass を実行しているデバイスからのセキュリティメトリッ	

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
			クスを、各デバイスで想定される動作からの逸脱がないか継続的に監視できます。	
CIP-007-6, R5	システムアクセスコントロール	Amazon Cognito AWS Directory Service AWS Managed Microsoft AD	電力事業者は、システムアクセス制御に関する既存のコンプライアンスプログラムに引き続き従うことができます。電力事業者は、既存のディレクトリサービス、AWS Directory Service または Amazon Cognito を使用して、インタラクティブなユーザー認証とアカウント管理をサポートできます。	
CIP-008-6, R1	インシデント対応プラン		電力事業者は、インシデント対応プランに関する既存のコンプライアンスプログラムに引き続き従うことができます。インシデントの検出と対応をサポートする AWS サービスの使用を組み込むように、インシデント対応プランを見直して更新する必要があります。	AWS はクラウドインフラストラクチャのセキュリティに責任を負い、クラウドインフラストラクチャのインシデント対応の統制に対処する複数の統制フレームワークへの準拠を実証しています。AWS のお客様はこれらの統制を引き継ぎ、AWS マネジメントコンソールのアーティファクトセクションで統制の有効性を示す保証レポートを参照できます。 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
CIP-008-6, R2	インシデント対応プランの実施とテスト	Amazon S3 AWS CloudTrail AWS CloudFormation Amazon CloudWatch	対応を支援するために、電力事業者は Amazon S3 上にデータレイクを作成し、AWS CloudTrail、その他の AWS サービス、Amazon CloudWatch、システムおよびアプリケーションログからのログを保存できます。その後、電力事業者は Amazon OpenSearch Service を使用してイ	

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
		Amazon OpenSearch Service AWS IoT Device Defender Amazon SNS	ベントログを分析し、インシデント調査活動に役立てることができます。AWS IoT Device Defender を使用して、AWS IoT または AWS IoT Greengrass を実行しているデバイスのセキュリティ調査を行うことができます。Amazon Simple Notification Service (Amazon SNS) を AWS IoT Device Defender と統合して、イベントに関する通知を即座に受け取ることができます。 インシデント対応プランとテストをサポートするために、電力事業者は AWS CloudFormation を使用してシステムのデプロイを自動化し、インシデント対応手順を迅速かつ低コストで、運用上のリスクをより低く、より頻繁にテストできる複製環境を作成する必要があります。	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. アクティベーションと通知フェーズ 2. 復旧フェーズ 3. 再構成フェーズ AWS のインシデント管理プランの有効性を確保するために、AWS はインシデントレスポンステストを実施しています。このテストにより、これまで知られていなかった欠陥や故障モードの発見を十分にカバーできます。さらに、Amazon のセキュリティチームとサービスチームは、潜在的なお客様への影響がないかシステムをテストし、検出と分析、封じ込め、根絶、復旧、インシデント後のアクティビティなどのインシデントに対処するためのスタッフをさらに準備できます。インシデント対応テストプランは、インシデント対応プランと併せて毎年実施されます。AWS のインシデント管理のプラン、テスト、およびテスト結果は、第三者の監査人が確認します。
CIP-008-6, R3	インシデント対応プランのレビュー、更新、コミュニケーション		電力事業者は、インシデント対応のレビュー、更新、コミュニケーションについて、既存のコンプライアンスプログラムに引き続き従うことができます。インシデントの検出と対応をサポートする AWS サービスの使用を組み込むように、インシデント対応プランを見直して更新する必要があります。	

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
CIP-008-6, R4	インシデント対応プランのレビュー、更新、コミュニケーション		電力事業者は、インシデントの通知と報告に関する既存のコンプライアンスプログラムのプロセスに引き続き従うことができます。インシデントの検出と対応をサポートする AWS サービスの使用を組み込むように、インシデント対応プランを見直して更新する必要があります。	
CIP-009-6, R1	復旧プラン、バックアップと復旧のプロセス、データ保存	AWS Backup AWS Elastic Disaster Recovery AWS CloudFormation	電力事業者は、復旧プラン、バックアップ、テストに関する既存のコンプライアンスプログラムのプロセスに引き続き従うことができます。電力事業者は、AWS でホストされているシステムについて、緊急時対応プラン、トレーニング、テストを適切に実施する責任を負います。バックアップと復旧のプロセスをサポートする AWS サービスの使用を組み込むように、復旧プランを見直して更新する必要があります。 AWS では、サーバーインスタンスの頻繁なバックアップの利用、データの冗長性複製、インスタンスの配置やデータの保存を複数の地域や各リージョン内の複数のアベイラビリティーゾーンに柔軟に行えるなど、堅牢な継続プランを実施する機能をお客様に提供しています。AWS Backup は、	AWS はクラウドインフラストラクチャのセキュリティに責任を負い、クラウドインフラストラクチャの復旧プランの統制に対処する複数の統制フレームワークへの準拠を実証しています。AWS のお客様はこれらの統制を引き継ぎ、AWS マネジメントコンソールのアーティファクトセクションで統制の有効性を示す保証レポートを参照できます。 AWS の事業継続プランには、障害発生時に AWS が従うプロセス (検出から非アクティブ化まで) が詳述されています。 AWS は、すべての AWS リージョンにわたってユビキタスなセキュリティコントロール環境を維持しています。各データセンターでは、物理的、

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
			AWS Storage Gateway を使用して、オンプレミスだけでなくクラウド内で AWS のサービス全体のデータのバックアップの一元化と自動化を簡単に実行できる、フルマネージド型のバックアップサービスです。	環境的、セキュリティ基準に基づいてアクティブ-アクティブ構成で構築されており、コンポーネントに障害が発生した場合のシステム可用性を確保するために冗長性を採用しています。
CIP-009-6, R2	復旧プランの実施とテスト	AWS Backup AWS Elastic Disaster Recovery AWS CloudFormation	AWS Elastic Disaster Recovery は、既存の物理データセンターまたは仮想データセンター、プライベートクラウド、またはその他のパブリッククラウドから迅速かつ簡単に災害復旧戦略を AWS クラウドに移行させる AWS サービスです。既に AWS に移行している場合は、クロスリージョンの災害復旧対策によってミッションクリティカルなワークロードをさらに保護することができます。 AWS CloudFormation を使用すると、電力事業者はシステムのデプロイを自動化できます。自動スケーリング、データバックアップ、自動デプロイの戦略により、手動で再構築するよりも大幅に短い時間で、システムを再構築して復旧作業をサポートできます。AWS クラウドは、シンプルなバックアップと復旧、パイロットライト、ウォームスタンバイ、マルチリージョンの常時稼働など、お客様の要	

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
			件に合わせて設定できる複数の災害復旧 (DR) のアーキテクチャをサポートしています。	
CIP-009-6, R3	復旧プランのレビュー、更新、コミュニケーション		電力事業者は、復旧プランの要件に関する既存のコンプライアンスプログラムのプロセスに従って、学んだ教訓を文書化したり、復旧プランを更新したり、特定の個人またはグループに更新を通知したりできます。	
CIP-010-3, R1 CIP-010-3, R2	ベースラインの設定と変更の管理 設定の監視活動	AWS Config AWS Systems Manager Amazon Inspector AWS Lambda Amazon SNS AWS CloudFormation	電力事業者は、設定変更管理と脆弱性評価に関する既存のコンプライアンスプログラムに引き続き従うことができます。AWS Config を使用すると、AWS 環境の変更を継続的に監視、評価、管理できます。AWS Config では、AWS リソースの設定の継続的な監視と記録が行われ、適切な設定に対する記録された設定の評価を自動化できます。AWS Config を使用すると、社内ガイドラインで指定されている設定に対する全体的なコンプライアンスを判断できます。これにより、コンプライアンス監査、セキュリティ分析、変更管理、運用のトラブルシューティングを簡素化できます。AWS CloudFormation を使用すると、セキュアなネットワーク、ストレージ、コンピューティングシステムの開発のためのテンプレートを開発して使用する	AWS はクラウドインフラストラクチャのセキュリティに責任を負い、クラウドインフラストラクチャの設定と脆弱性管理の統制に対処する複数の統制フレームワークへの準拠を実証しています。AWS のお客様はこれらの統制を引き継ぎ、AWS マネジメントコンソールのアーティファクトセクションで統制の有効性を示す保証レポートを参照できます。 AWS は変更を管理するための体系的なアプローチを採用し、本稼働環境におけるすべての変更が確実にレビュー、テスト、承認されるようにしています。

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
			こともできます。 お客様は、AWS Inspector と AWS Systems Manager を使用して、AWS 環境内にデプロイされたシステムに設定されたベースライン標準を監視することもできます。	
CIP-010-3, R3	脆弱性評価と修復		お客様は、サードパーティ製の脆弱性評価ツールを使用して AWS 上のサーバーをスキャンできます。これらのツールの多くは、AWS Marketplace から直接入手してデプロイできます。	AWS セキュリティは、システム境界内でセキュリティ関連のアクティビティを実施する場合、適切なサービスチームに通知し、調整します。アクティビティには、脆弱性スキャン、緊急時対応テスト、インシデント対応の演習が含まれます。AWS は、外部からの脆弱性評価を少なくとも四半期に一度実施し、特定された問題を調査して解決まで適時追跡します。さらに、AWS は、独立した第三者にシステム内の防御とデバイス設定を調査してもらうことにより、予告なしに侵入テストを実施します。
CIP-010-3, R4	一時的なサイバーシステムとリムーバブルメディアの管理		電力事業者は、TCA (Transient Cyber Assets) の使用に関する既存のコンプライアンスプログラムに引き続き従うことができます。	AWS はクラウドのセキュリティに責任を負い、FedRAMP を含むいくつかの規制コンプライアンス要件を満たしています。AWS では、インフラストラクチャを保護するために FedRAMP/NIST

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
				AC-17 から 20 を含むセキュリティコントロールを実装しています。
CIP-011-2, R1	BCSI の識別と保護	AWS KMS	電力事業者は、情報保護要件に関する既存のコンプライアンスプログラムに引き続き従うことができます。 Access Analyzer for S3 などの機能は、AWS アカウントの外部から Amazon S3 のコンテンツにアクセスできる場合は直ちに責任者に警告し、作成中のバケットのアクセスポリシーを評価するのに役立ちます。	AWS はクラウドインフラストラクチャのセキュリティに責任を負い、クラウドインフラストラクチャの情報保護に関する統制に対応する複数の統制フレームワークへの準拠を実証しています。AWS のお客様はこれらの統制を引き継ぎ、AWS マネジメントコンソールのアーティファクトセクションで統制の有効性を示す保証レポートを参照できます。
CIP-011-2, R2	サイバーシステムの再利用または廃棄前の BCSCI のサニタイズ	AWS IAM AWS KMS AWS CloudTrail	電力事業者は、転送中および保存中のデータを暗号化できます。Amazon EBS、Amazon RDS、Amazon DynamoDB、Amazon S3 などの AWS のストレージサービスでは、保存中のデータを暗号化できます。電力事業者は IAM ポリシーを使用してデータへのユーザーアクセスを制御し、AWS Key Management Service (KMS) を使用して保存中のデータを暗号化できます。	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、お客様の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 では、運用停止プロセスの一部に、「メディアのサニタイズ」に関する NIST SP800-88 のガイドラインに記載された手法を適用しています。 ドライブ上のコンテンツは、AWS ポリシーに従って最高レベルの分類で処理されます。コンテンツは、AWS のセキュリティ基準に従って廃

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
				棄プロセスの一環としてストレージデバイス上で破棄されます。AWS のホストは、プロビジョニング前に安全に消去または上書きされて再利用されます。AWS のメディアは、AWS のセキュアゾーンを出る前に安全に消去または消磁処理され、物理的に破壊されます。
大規模環境でのガバナンス	CIP 統制の管理と実装に役立つ AWS のサービス	AWS Audit Manager AWS Control Tower AWS Security Hub AWS Organizations	電力事業者は、「大規模なガバナンス」と呼ばれる、大規模なクラウドシステムの管理に役立つ複数の AWS サービスを使用できます。 AWS Control Tower は、数回クリックするだけでマルチアカウントの AWS 環境のセットアップを自動化するサービスです。セットアップにはブループリントを使用し、これには AWS のセキュリティおよび管理サービスを設定するための AWS のベストプラクティスを収めています。ブループリントは、アイデンティティ管理、アカウントへのフェデレーションアクセス、統合ログ管理、クロスアカウントのセキュリティ監査の確立、アカウントのプロビジョニング用ワークフローの定義、ネットワーク設定でのアカウントベースラインの実装に使用できます。	

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
			AWS Organizations は、環境の一元管理とガバナンスを支援します。AWS Organizations を使用して、電力事業者は新しい AWS アカウントをプログラムで作成してリソースを割り当てる、アカウントをグループ化してワークフローを整理する、アカウントやグループにポリシーを適用してガバナンスを確保する、すべてのアカウントの支払い方法を一本化して請求を簡素化するなどの処理を行うことができます。例えば、電力事業者は対象範囲のワークロード用にアカウントのグループを作成し、これらのアカウントに共通のポリシーと制御を設定できます。 電力事業者は AWS Security Hub を使用して、AWS アカウント/組織全体のセキュリティアラートと態勢を包括的に把握できます。AWS Security Hub により、電力事業者は複数の AWS のサービス (Amazon GuardDuty、Amazon Inspector、AWS Identity and Access Management (IAM) Access Analyzer、AWS Systems Manager、AWS Firewall Manager など) および AWS パー	

CIP 標準要件の目標	CIP 標準の説明	AWS のサービス	お客様に関する考慮事項	AWS の責任
			トナーネットワーク (APN) のソリューションでのセキュリティアラートと検出結果を、一元的に集約、整理、優先順位付けできるようになります。 電力事業者は AWS Audit Manager を使用して、AWS の使用状況を継続的に監査して、リスクの査定や、規制および業界規格への準拠状況の評価を容易に行うことができます。 AWS Audit Manager の使用によって証跡収集を自動化し、監査時に行われがちな「全員参加型」の手作業を減らすとともに、クラウドでの監査機能を拡張できます。AWS Audit Manager を使用すると、ポリシー、手順、および活動 (統制とも呼ばれる) が効果的に機能しているかどうかを簡単に評価できます。監査の際には、AWS Audit Manager を使用すれば、ステークホルダーによる統制のレビューを管理しやすくなり、手作業を大幅に減らして監査用のレポートを作成できます。	