AWS における NERC CIP 大規模電力システムサイバーシステム情報 (BCSI: BES Cyber System Information) 対応

コンプライアンスガイド

2023 年 2 月 2 日

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。

目次

要約

このホワイトペーパーは、North American Electric Reliability Corporation (NERC) に大規模電力システムのユーザー、所有者、および運営者として登録されている、また重要インフラストラクチャーの保護 (CIP) 規格の対象であり、Amazon Web Services (AWS) 上の大規模電力システムサイバーシステム情報 (BCSI) を保護する管理を実施する責任を負っている電力事業者を対象としています。

このホワイトペーパーでは、CIP-004-7 Cyber Security - Personnel & Training と CIP-011-3 Cyber Security - Information Protection の要件に適合する AWS の統制を特定し、AWS クラウドで BCSI をホストし保護するための NERC CIP 準拠アーキテクチャの設計とデプロイに役立つセキュリティのベストプラクティスとアーキテクチャの推奨事項を提供します。

概要

このホワイトペーパーでは、電力事業者とパートナー向けに、AWS クラウドで BCSI の保護に役立つソリューションを設計およびデプロイする方法について、概要的なガイダンスを提供します。電力事業者は、AWS 上で CIP-004-7 と CIP-011-3 に該当する要件を満たすためにさまざまな設計パターンを使用できますが、この文書では、より一般的なユースケースの多くに対応できるサンプルリファレンスアーキテクチャを紹介します。

この文書は、情報技術 (IT) の責任者、運用技術 (OT) の責任者、コンプライアンスの責任者、そしてセキュリティ担当者を対象としています。ネットワーク、データ暗号化、運用管理の分野における基本的なセキュリティ概念に精通していることを前提としています。

大規模電力システム (BES) のサイバーシステム情報 (BCSI) に関する NERC CIP 規格要件の目的は、BES サイバーシステムに不正アクセスやセキュリティ上のリスクをもたらすために使用される可能性のある情報を保護することにあります。不正アクセスや漏洩によって機密性が損なわれるリスクを軽減するためには、BCSI を特定し、保護し、安全に取り扱わなければなりません。コンプライアンスを達成するためには、電力事業者は必要な統制を実施するための計画を立て、CIP-004-7 および CIP-011-3 で特定された NERC CIP BCSI 要件の適合を実証するために必要な証拠を収集し維持する必要があります。

2021 年 12 月、連邦エネルギー規制委員会 (FERC) は、NERC の 2 つの CIP 規格である CIP-004-7 と CIP-011-3 の改訂を承認しました。改訂された規格により、BCSI を保護するための CIP 要件が変更され、クラウド技術を含む最新のサードパーティデータストレージおよび分析システムに安全かつ規制当局の承認を受けた方法が提供されるようになりました。これらの変更により、クラウド技術の使用に関するこれまでのコンプライアンス上の懸念が解決され、電力事業者が適切なコンプライアンス統制を実施し、コンプライアンスの監視および実施プロセスでそれを実証できる限り、BCSI をクラウドに保管、送信、使用できるようになります。

AWS 自体は大規模電力システムの所有者でも運営者でもないため、NERC CIP 規格の対象ではありません。クラウドサービスのための NERC CIP 認証プログラムは存在しませんが、AWS は FedRAMP や System and Organization Control (SOC) など、NERC CIP 規格の対象となる電力事業者にとって特に興味深いと思われる複数の規制や認証フレームワークへの準拠を実現しています。

背景

AWS は、電力事業者が BES の信頼性を高めるために、BCSI を管理するための選択肢の拡大、柔軟性の向上、可用性の向上、コストの削減に関心を持っていることを認識しています。クラウドソリューションは、信頼性の高いオペレーションを継続するための業界イノベーションに対して重要な位置付けとなっています。 NERC の FERC への報告書類に次の記述があります。

> 「...テクノロジーが進化するにつれて、クラウドサービスなどのサードパーティサービスが、BCSI を保管するための実用的で安全な選択肢になってきました。たとえば、責任のある電力事業者がクラウドにある情報を保護するために利用できる保護手段は、情報の実際の保管場所よりも、ファイルレベルの権限と許可に大きく依存します」

承認された実施計画によると、改訂された規格は 2024 年 1 月 1 日に施行されますが、施行日より前に採用することが可能です。

改訂された規格に加えて、電力事業者は NERC 電気信頼度機関 (ERO) が作成した BCSI およびクラウドガイダンス文書を参照できます。これらの文書には、クラウド環境にある BCSI のためのより具体的な推奨事項が記載されています。たとえば、「Security Guideline for Electricity Sector - Primer for Cloud Solutions and Encrypting BCSI」には、クラウド環境で BCSI へのアクセスを保護および制限する手段として暗号化を使用する方法に関するガイダンスが記載されています。「ERO Enterprise CMEP Practice Guide: BES Cyber System Information」は、指定の BCSI 保管場所へのアクセスを許可する電力事業者のプロセスを評価する監査人にガイダンスを提供しています。

過去長い間、電力事業者は BCSI をクラウド環境に移行することを検討してきましたが、適用される CIP 規格を遵守することに苦労していました。規制当局も機密情報のクラウドへの移行を承認することをためらっていました。改訂された規格と関連する NERC ガイダンスのおかげで、これらの問題を解決し、当局の期待を満たす方法で BCSI を使用できるようになったのです。

はじめに

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。BCSI のクラウド移行を成功させるには、電力事業者が組織の現在の状態や目標、その目標を達成するために必要な過程などを理解しておくことが重要です。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。

「AWS Power and Utility Path to Production in the Cloud」は、カスタマージャーニーを管理しやすいパーツに分解し、電力事業者が必要とする人材、義務、必要なリソースを考慮してクラウドソリューションを実装する方法を考えるのに役立ちます。

この移行を計画するには、電力事業者は、移行前、移行中、移行後の BCSI の安全性を示せるような方法で規制当局に変更を提示する必要があります。NERC および電力事業者の CIP 規格への準拠を評価する監査チームと協力することは、電力事業者のコンプライアンスプログラムに対する監査人の信頼を得るために重要です。規制当局の視点とそれに必要な透明性を考慮すると、電力事業者のスタッフがクラウドで活躍できるようにするための目標を設定し、移行のためのワークフローを構築するのに役立ちます。また、準拠を実証するために必要な証拠の作成と維持に役立ち、BCSI が AWS クラウドで保護されていることを監査人が確認するのに必要な高いレベルの保証を提供するのにも役立ちます。

はじめに、以下の技術とコンプライアンスに関する質問の回答内容を検討する必要があります。

- AWS クラウドは NERC CIP コンプライアンスプログラム準拠を効果的に対応することができますか？
- AWS クラウドを使用することで、セキュリティ、ロギング、モニタリング、インシデント対応という目標をどう達成できますか?
- 可視性、信頼性、またはセキュリティの向上で恩恵を受けるアプリケーションやシステムはありますか?
- コンピューティング、ストレージ、ネットワークの容量要件はどのようなものですか?
- プログラムをサポートするためにスケールアップ (またはスケールダウン) をどのように準備していますか？

これらの質問を検討する際には、柔軟性、費用対効果、スケーラビリティ、伸縮性、セキュリティといった観点を念頭に置きつつ、コンプライアンスを実証する能力を維持することも重視しましょう。AWS のサービスを利用することで、自分たちのコアコンピテンシーに集中でき、AWS が提供するリ

ソースや経験を NERC CIP 規格に沿った方法で活用でき、監査ではコンプライアンスの証明もしやすくなります。

責任とガバナンスの共有

図 1 にあるように、セキュリティは AWS と電力事業者の共有責任になっています。この共有モデルでは、ホストオペレーティングシステムならびに仮想化レイヤーからサービスを実行する施設の物理的なセキュリティに至るまでのコンポーネントを AWS が運用、管理、統制するため、運用に伴う電力事業者の負担が軽減されます。

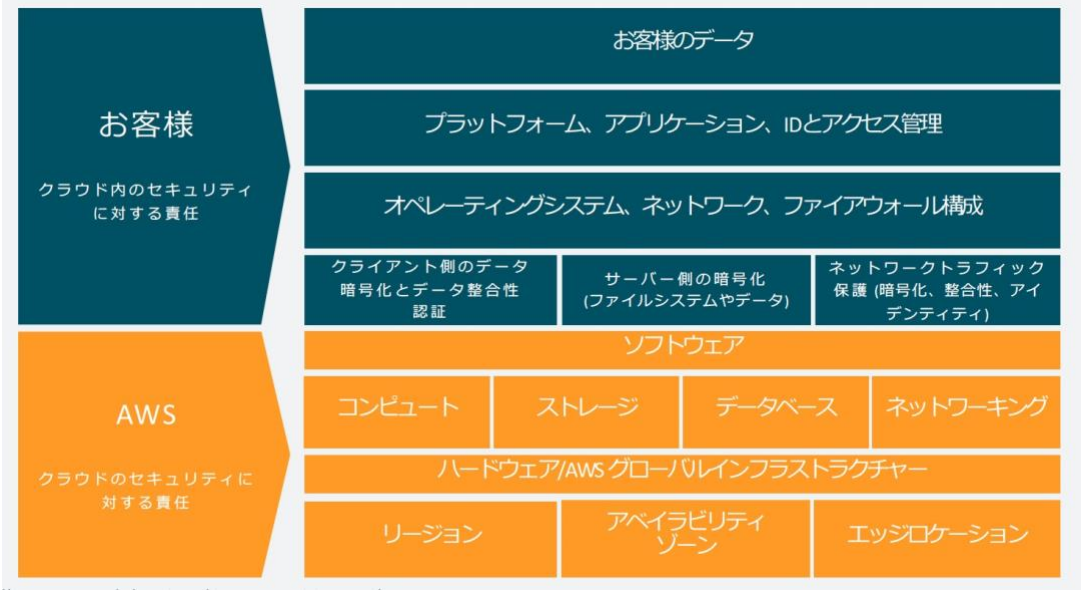

図 1: AWS 責任共有モデル

電力事業者は、ゲストオペレーティングシステム (更新やセキュリティパッチなど)、その他の関連アプリケーションソフトウェア、ならびに AWS より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に対する責任とその管理を引き受けます。電力事業者の責任範囲は、使用するサービス、自社 IT 環境へのサービス統合、適用される法律や規制に応じて異なってきます。そのため、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。

責任共有モデルはコンプライアンス統制にも適用されます。環境を運用する責任が AWS と電力事業者の間で共有されるように、共有されたコンプライアンス統制の管理、運用、保守、検証も共有されます。

責任共有モデルは選択したソリューションによって異なる可能性があるため、BCSI 用の AWS パートナーソリューションを使用する電力事業者は、それが自社固有のユースケースにどのように適用されるか検討する必要があります。

適用される NERC ガイダンスにより、NERC 機能の遂行を担当する NERC 登録電力事業者は、その機能に適用される信頼性基準の遵守について単独で責任を負います。特定の業務の遂行が第三者または第三者が提供するサービスに依存している場合でも同様です。したがって、責任共有モデルは AWS と電力事業者間での管理、運用およびセキュリティ統制の分担を示していますが、NERC CIP 規格に基づくコンプライアンス義務が電力事業者から AWS に移行したり、AWS が電力事業者のコンプライアンス責任や賠償責任を引き受けることを要求または示唆したりするものではありません。

継承統制、共有統制、電力事業者固有の統制

責任共有モデルをさらに明確にするために、統制は「継承統制」、「共有統制」、「電力事業者固有の統制」の 3 つのカテゴリに分類されます。

継承統制とは、電力事業者が AWS から物理統制と環境統制を含め完全に継承する統制です。AWS は、AWS クラウド内で提供するすべてのサービスを実行するインフラストラクチャーである AWS **クラウドの**セキュリティとコンプライアンスに責任を持ちます。このインフラストラクチャーは、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。これには、電力事業者リソースとデータを論理的に分離する統制、AWS データセンターの物理的なセキュリティ、その他の管理、コンプライアンス、セキュリティ関連の統制が含まれます。

電子的な BCSI を保護するための物理的なセキュリティ統制は NERC CIP 規格で直接義務付けられているわけではありませんが、AWS の物理インフラストラクチャーに関連するセキュリティ統制は AWS が管理しています。電力事業者は AWS Artifact で手に入る AWS の統制およびコンプライアンスに関するドキュメントを使用して、統制の評価および検証手順を実行できます。

共有統制はインフラストラクチャーレイヤーと電力事業者レイヤーの両方に適用されますが、コンテキストや視点はまったく異なります。統制共有では、AWS がインフラストラクチャーに対する要求事項を提供し、電力事業者は AWS のサービスの使用に対して独自の統制を実装する必要があります。統制共有は、セキュリティ義務またはコンプライアンス義務の移転を意味するものではありません。むしろ、AWS と電力事業者の双方が、セキュリティ目標を達成するためにそれぞれの統制を実施する必要があります。次の例が挙げられますが、これらに限定されるものではありません。

- パッチ管理 - AWS はインフラストラクチャーのパッチ適用と保守を担当しますが、電力事業者は利用する AWS 環境内のゲストオペレーティングシステムとアプリケーションにパッチを適用する責任を負います。
- 構成管理 - AWS がインフラストラクチャーデバイスの構成を保守しますが、電力事業者は利用する AWS 環境内の独自のゲストオペレーティングシステム、データベース、アプリケーションの構成に責任を負います。

個々の電力事業者の要件にあった統制活動については、電力事業者が AWS にデプロイするアプリケーションに基づいて単独で責任を負います。電力事業者の責任は、電力事業者が選択する AWS クラウドサービスによって決定されます。これにより、電力事業者がセキュリティの責任の一部として実行する必要がある設定作業の量が決まります。

次の例が挙げられますが、これらに限定されるものではありません。

- サービスおよびコミュニケーション保護またはゾーンセキュリティでは、電力事業者が特定のセキュリティ環境下でデータのルーティングやゾーニングを行わなければならない場合があります。
- データを保護するための暗号化の設定に責任を負います。
- ユーザーアカウントとロールの ID とアクセス権限の設定と保守管理に責任を負います。
- Amazon Elastic Compute Cloud (Amazon EC2) インスタンスをデプロイする電力事業者は、ゲストオペレーティングシステム (アップデートやセキュリティパッチを含む) とインスタンスにインストールされるソフトウェアの管理に責任を負います。
- Amazon Simple Storage Service (Amazon S3) や Amazon DynamoDB などの抽象化サービスの場合、電力事業者はデータ (暗号化オプションを含む) を管理し、アセットとリソースを分類し、IAM ツールを使用して適切なアクセス統制と権限を適用する責任を負います。

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場合は、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 サポート

AWS サポートでは、電力事業者の AWS ソリューションの成功と運用状態をサポートするツールや専門知識にアクセスしやすくするための幅広いプランを提供しています。すべてのサポートプランでは、カスタマーサービス、AWS 文書、テクニカルペーパー、およびサポートフォーラムを 24 時間年中無休でご利用いただけます。24 時間年中無休のオンデマンドテクニカルサポートを利用すると、規制当局からの問い合わせに対応するために必要な情報を収集できます。コンプライアンスの監視活動および対応において、AWS の担当者は対象分野の監視担当としての役割を果たすことはできませんのでご注意ください。

AWS サポートでは、Basic、Developer、Business、Enterprise On-Ramp、Enterprise の 5 つのサポートプランを提供しています。電力事業者はニーズに応じた AWS サポートプランを比較できます。Enterprise On-Ramp プランと Enterprise プランでは、電力事業者へのプロアクティブなガイダンスや最適化支援、またプログラムへのアクセスを調整するために使用できるテクニカルアカウント管理を提供します。AWS 環境の計画、デプロイ、改善のためのテクニカルサポートやその他のリソースについては、電力事業者はそれぞれの AWS ユースケースに最も合ったサポートプランを選択できます。

適用範囲と BES サイバーシステム情報 (BCSI) 環境

NERC 用語集は、BCSI を次のように定義しています。

> 「BES サイバーシステムに、不正アクセスやセキュリティ上の脅威をもたらすために使用される可能性のある BES サイバーシステムに関する情報を、BES サーバーシステム情報 (BCSI) と定義しています。BES サイバーシステム情報には、デバイス名、コンテキストを含まない個々の IP アドレス、ESP 名、ポリシーステートメントなどの、単独では脅威とならない、または BES サイバーシステムへの不正アクセスを許可するために使用できない個々の情報は含まれません。BES サイバーシステム情報の例としては、BES サイバーシステムについてのセキュリティ手順またはセキュリティ情報、物理アクセス制御システム、一連のネットワークアドレスおよび BES サイバーシステムのネットワークトポロジーなど公開されておらず不正アクセスまたは不正配布を許可するために使用される可能性がある電子アクセス制御または監視システムなどがあります」

BCSI 適用範囲の決定

電力事業者は、BCSI を特定する方法を含む BCSI の情報保護プログラムを 1 つ以上文書化する責任を負っています。電力事業者は、自社の情報保護プログラムに従って、BCSI として分類されるデータを決定する責任を負っています。データには、NERC CIP アセットデータベース、運用中のテクノロジーネットワークのデータ、ネットワーク図、NERC CIP コンプライアンスエビデンス、およびその他の機密情報が含まれる場合があります。

クラウド環境に置かれているものを含むオフプレミスの電子的 BCSI は、電子技術的方法 (暗号化、ハッシュ、トークン化、電子鍵管理など)、管理方法 (ベンダーサービスリスク評価や業務契約など)、ID 管理とアクセス管理の実装を通じて保護される必要があります。

電力事業者は環境内で BCSI の範囲を特定し、その BCSI を保護するために実施されているコンプライアンス統制を監査人が検証できるようにする必要があります。

AWS での NERC CIP BCSI 適合に関するガイド

このセクションでは、電力事業者が AWS サービスを使用して BCSI を保護する方法に関するガイダンスを提供します。BCSI に適用される CIP-004-7 および CIP-011-3 要件により、各電力事業者は要件の文言に準拠するプログラムと方法を定義できます。このセクションではプログラムの機能と統制に関する推奨事項を紹介しますが、各電力事業者には、NERC CIP 規格に基づくコンプライアンス義務に照らして選択肢を評価し、適切と思われる統制を実施する責任があります。

責任共有と継承された統制、および特定の CIP 規格と要件への準拠をサポートするために AWS サービスをどのように使用できるかについては、「付録 1: AWS のサービスと NERC CIP への適合」の表を参照してください。

CIP-011-3 要件 1 - 情報保護プログラム

CIP-011-3 要件 1 は、電力事業者に対し、該当するシステムに関する文書化された情報保護プログラムを実施することを要求しています。情報保護プログラムには、BCSI を特定する方法 (パート 1.1) と、BCSI を保護し安全に扱う機密性が損なわれるリスクを軽減する方法 (パート 1.2) を含める必要があります。

CIP-011-3 要件 1 パート 1.1 - BCSI を特定する方法

AWS クラウドでは、電力事業者は BCSI の保管と処理に関連するリソースを特定して一覧表示することができます。1 つの方法は、BCSI に関連する各リソースに AWS タグを割り当てるものです。もう 1 つの方法は、特定の AWS アカウントを BCSI 専用にするものです。

BCSI 用の AWS タグ

電力事業者は、BCSI を含む AWS リソースにタグを付けることができます。タグはユーザーが定義したキーと値で構成されるラベルです。タグは、リソースの管理、特定、整理、検索、フィルター処理に役立ちます。タグを作成して、目的、所有者、環境、またはその他の基準でリソースを分類できます。

タグは AWS リソースに関する以下の情報を特定できます。

- リソースに BCSI が保管されているかどうか
- セキュリティ詳細 (例: 暗号化の種類と強度、トークン化、アクセス統制、切り捨て)
- BCSI が関係する該当するシステム (例: BES サイバーシステム、電子アクセス統制または

監視活動システム、または BES サイバーシステムに関連する物理アクセス統制システム)

- BCSI が関係する該当システムの影響評価 (例: 影響大または中程度)

図 2 は、Amazon EC2 インスタンスにアタッチされた Amazon Elastic Block Store (Amazon EBS) ボリュームの AWS タグの例を示しています。このタグは、電力事業者が NERC CIP BCSI を特定するために使用する場合があります。

Key	Value
Compliance	BCSI
Encryption Strength	256
Impact Rating	High
Key Management	aws-kms
Name	my-data-server

図 2: Amazon EC2 インスタンスにアタッチされた Amazon EBS ボリュームの AWS タグの例

電力事業者は AWS Resource Groups を使用して、BCSI に関連するリソースを含め、同じ AWS リージョンにある AWS リソースを整理および管理できます。Resource Groups を使用すると、電力事業者は AWS リソースのグループに対して、セキュリティパッチや更新の適用などのタスクを同時に自動化できます。

図 3 は、AWS マネジメントコンソール内の Resource Groups と、電力事業者が BCSI としてタグ付けされたリソースを表示する方法を示しています。

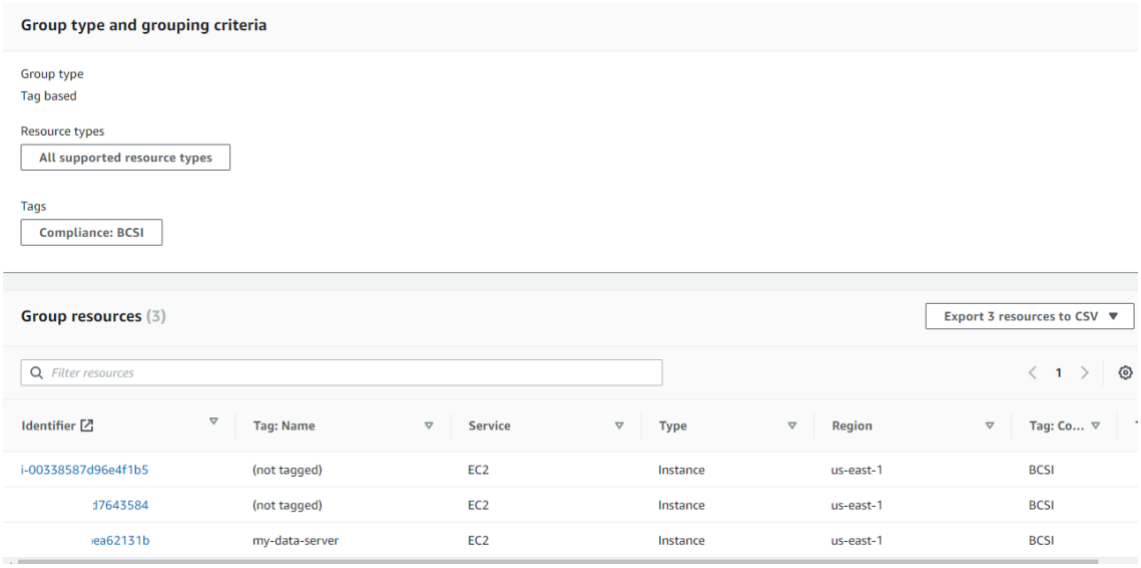

図 3: AWS Resource Groups

AWS Config を使用すると、電力事業者は関連するタグ値を使用してリソースをクエリできます。電力事業者はこのサービスを使用して、AWS リソースの設定を調査や監査、または評価することができます。AWS Config では、AWS リソース設定を継続的に監視および記録し、電力事業者の理想的な設定と比較した場合の記録された設定の評価を自動化することができます。

AWS Config を使用すると、電力事業者は AWS リソース間の設定や関連性の変更を確認し、詳細なリソース設定履歴を調べ、内部ガイドラインで指定された設定に対する全体的なコンプライアンスを決定できます。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、運用上のトラブルシューティングを簡素化できます。

BCSI 専用アカウント

AWS ではマルチアカウント戦略を推奨しています。これには、電力事業者が AWS Control Tower を使用して管理および運用できる、BCSI にアクセスするための専用アカウント (1 つあるいは複数) が含まれます。電力事業者はこれらの専用アカウントのリソースを BCSI として分類できるため、手動でリソースを特定してタグ付けする必要を減らせ、専用アカウントの BCSI に継続したセキュリティ統制を確実に適用できるようになります。

AWS Control Tower を使用すると、電力事業者は**ランディングゾーン**と呼ばれる安全なマルチアカウントの AWS 環境をセットアップして管理できます。AWS Control Tower は AWS Organizations を使用してランディングゾーンを作成します。AWS Organizations は、プログラムによる新しい AWS アカウントの作成とリソースの割り当て、アカウントのグループ化によるワークフローの整理、ガバナンス目的でのアカウントまたはグループへのポリシーの適用、すべてのアカウントに 1 つの支払い方法を使うことによる請求の簡素化を可能にします。

AWS Organizations は、電力事業者が一元的な設定、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。

図 4 は、電力事業者が AWS Organizations を使用して責任分担を実装する方法の例を示しています。この例では、エンタープライズシステムは業務とは異なる組織単位に分割されています。

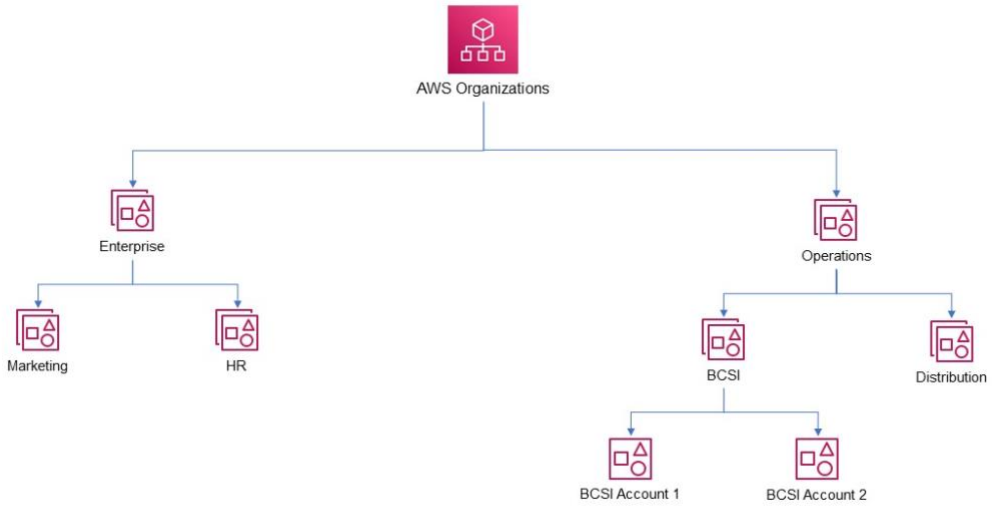

図 4: AWS Organizations の例

電力事業者は、会社のポリシーに準拠する新しい AWS アカウントを規定したり、ガバナンスを新規または既存のアカウントに拡張したり、コンプライアンスステータスを可視化したりできます。

CIP-011-3 要件 1 パート 1.2 - 電子的 BCSI を保護し、安全に扱うための電子技術的方法

CIP-011-3 要件 1 パート 1.2 では、BCSI を保護して安全に扱うための特別な方法は必要ありません。代わりに、クラウド環境のストレージを使用することで、電力事業者は、データマスキング、暗号化、ハッシュ、トークン化、暗号化、鍵管理など、さまざまな電子的方法を使用して BCSI を保護できます。以下のセクションで説明するように、AWS には電力事業者が監査可能な方法でこれらの目的を達成するために使用できるツールが多数用意されています。

論理的な分離

データを論理的に分離することは、電子的 BCSI を保護するための電子技術的方法の実装と実証の基礎となる要素です。電力事業者に AWS Control Tower またはランディングゾーンソリューションを使用した確立された AWS 環境がある場合は、BCSI 専用のアカウントを作成できます。また事業者が一部の BCSI を移動した、または利用している既存の AWS アカウントを持っている場合や、事業者が新しい AWS アカウント環境を構築している場合もあるかもしれません。いず

れのシナリオでも、BCSI を保護するための電子技術的な方法には、AWS サービスを使用してデータを論理的に分離することが含まれます。

Amazon Virtual Private Cloud (Amazon VPC) を使用すると、電力事業者は AWS クラウドの論理的に分離されたセクションを規定し、定義した仮想ネットワーク内で AWS リソースを起動できます。

デフォルトでは、VPC は分離されたネットワークであり、VPC 内のサブネットにデプロイされたリソースは、別の AWS アカウントや VPC、パブリックインターネット、電力事業者のデータセンターなど、VPC 外のリソースとはコミュニケーションできません。電力事業者は、オンプレミスのデータセンターとの通信を許可するように VPN ゲートウェイとサブネットルートテーブルを設定する必要があります。電力事業者は、ニーズに合わせて選択および構成したゲートウェイを使い、環境のコミュニケーションリンクを決定します。

セキュリティグループは Amazon VPC 内のリソースのステートフル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の両方を統制します。電力事業者はセキュリティグループを使用して、IP アドレス、ポート、プロトコルでトラフィックを制限したり、CIP-011-3 要件 1 パート 1.2 の要素をサポートしたりできます。

ネットワークアクセスコントロールリスト (ネットワーク ACL) は、1 つ以上のサブネットを出入りするトラフィックを統制するためのステートレスルーターとしての役割を果たす、VPC 用のオプションのセキュリティ層です。ネットワーク ACL を使用する電力事業者は、接続ソース (標準 CIDR IPv4 または IPv6 形式) や特定の AWS リソースに基づいてトラフィックを評価および拒否し、オープンシステム相互接続 (OSI) モデルのレイヤー 4 より上のトラフィックフィルタリングを行うことができます。

VPC エンドポイントは、電力事業者の VPC 内のプライベート IP アドレスを使用してサポートされている AWS サービスに接続できる Amazon VPC の機能です。VPC エンドポイントは、AWS PrivateLink によるサービスです。このトラフィックは AWS ネットワークを離れることがなく、インターネットアクセスやパブリック IP アドレスを必要とせず VPC エンドポイントで公開されるリソースとコミュニケーションすることができます。

電力事業者は、AWS パートナーが AWS Marketplace を通じて提供しているサードパーティファイアウォールソフトウェアを使用して、AWS と電力事業者のオンプレミス環境に包括的なセキュリティアーキテクチャとシームレスなエクスペリエンスをデプロイすることができます。

AWS NERC CIP BCSI リファレンスアーキテクチャの実例については、「付録 2: AWS NERC CIP BCSI リファレンスアーキテクチャ」を参照してください。

転送時の暗号化

AWS は、電力事業者が Amazon VPC に安全に接続するための方法を提供しています。仮想プライベートネットワーク (VPN) ソリューションは、電力事業者のオンプレミスネットワーク、リモートオフィス、クライアントデバイス、AWS グローバルネットワーク間の安全な接続を確立するのに役立ちます。AWS VPN は、AWS Site-to-Site VPN と AWS Client VPN の 2 つのサービスで構成されています。各サービスは、ネットワークトラフィックの保護に役立つ、可用性が高く、暗号化された、柔軟なマネージドクラウド VPN ソリューションを提供します。

帯域幅と高いパフォーマンスを確保するために、電力事業者は AWS Direct Connect デリバリーパートナーと協力して、 MAC セキュリティ (MACsec) (IEEE 802.1AE) をサポートする AWS への専用ファイバー接続である AWS Direct Connect を実装できます。AWS Direct Connect は、10 ギガビット/秒 (Gbps) および 100 Gbps リンクのネイティブなラインレートに近いポイントツーポイント暗号化を実現します。

電力事業者が所有するサーバー間、または電力事業者とサードパーティが所有するサーバー間の通信を保護するには、電力事業者は SSL/TLS を使用する必要があります。AWS Certificate Manager (ACM) を使用することで、電力事業者は AWS サービスと内部接続リソースで使用するパブリックおよびプライベート SSL/TLS 証明書を規定、管理およびデプロイすることができます。

SSL/TLS 証明書は、ネットワーク通信を保護し、プライベートネットワーク上のリソースだけでなく、インターネットでウェブサイトの ID を確立するために役立ちます。ACM を使用することで、SSL/TLS 証明書の購入、アップロード、および更新という時間のかかるプロセスを手動で行う手間を減らせます。

電力事業者は、米国東部/西部リージョンまたは AWS カナダ (中部) リージョンにアクセスするときには、コマンドラインインターフェイス (CLI) を使用して、または AWS 提供の FIPS エンドポイントを使用してプログラム的に FIPS 140-2 で検証された暗号化モジュールを使用できます。これにより、セキュリティやコンプライアンスのニーズに対応できます。

保管時の暗号化

AWS Key Management Service (AWS KMS) は、他の AWS サービスと統合され、保管中のデータを暗号化したり、AWS KMS キーを使用して署名や検証を容易にしたりします。保管中のデータを保護するには、統合された AWS のサービスでエンベロープ暗号化を使用します。この暗号化ではデータキーが使用され、データキー自体が AWS KMS に保管されている KMS キーに基づいて暗号化されます。署名や検証にあたっては、統合された AWS のサービスでは、AWS KMS の非対称 KMS キーのキーペアを使用します。統合されたサービスで AWS KMS を使用する方法の詳細については、AWS のサービスに関するドキュメントをご覧ください。

暗号化を設定し、強力なデータ保持ポリシーと手順を維持するのは電力事業者の責任です。電力事業者は AWS KMS か AWS CloudHSM、またはその両方を使用して、要件 1 パート 1.2 に含まれるキーマテリアルの作成と管理に役立てることができます。IAM を使用するときめ細かなアクセス制限を適用できます。

鍵管理

電力事業者は AWS KMS か AWS CloudHSM、またはその両方を使用して、多くのキー管理要件のコンプライアンス負担を軽減できます。クラウドネイティブなアプローチに移行し、クラウドワークロードの暗号化を最適化し、自己管理型の HSM と比較して管理上の負担を軽減したいと考えているお客様には、電力事業者は AWS KMS を選択するべきです。AWS KMS を使用すると、電力事業者は KMS キーを安全に作成、保管、管理できます。電力事業者の KMS キーが AWS KMS を暗号化しないままにすることはありません。電力事業者は AWS KMS でキーポリシーを作成および管理して、信頼できるユーザーのみが KMS キーにアクセスできるようにすることもできます。KMS キーは、AWS KMS が管理する FIPS 検証済みの**ハードウェアセキュリティモジュール** (HSM) によって裏付けられています。HSM は、暗号化されたキーを生成して保管する特殊なセキュリティデバイスです。

AWS KMS のセキュリティと品質管理は、AWS システムおよび組織統制 (SOC 1、SOC 2、SOC 3)、FIPS 140-2 レベル 3、および FedRAMP のコンプライアンス体制によって検証および認定されています。

電力事業者は、キーポリシーと IAM ポリシーで AWS KMS キー管理機能へのアクセスを統制する責任があります。AWS KMS を使用すると、電力事業者は KMS キーを完全に制御できます。これには、キーポリシー、IAM ポリシー、権限付与の確立と管理、KMS キーの有効化と無効化、暗号化マテリアルのローテーション、タグの追加、KMS キーを参照するエイリアスの作成、KMS キー削除のスケジューリングなどが含まれます。 AWS KMS は他の AWS サービスとネイティブに統合されます。

AWS KMS は、カスタマーマネージドキー、AWS マネージドキー、カスタマーインポートキーの

3 種類のキーをサポートしています。カスタマーマネージドキーは、AWS KMS を使用するお客様によって生成、所有、管理されます。AWS マネージドキーは、自動化と AWS サービスとの統合を利用して、電力事業者がサービスに暗号化を指示すると、AWS がキーを生成して暗号化できるようにします。ここからは、電力事業者はキーを使用して AWS KMS のメリットを享受できます。

3 番目のオプションは、お客様が別の HSM によって生成されたキーをインポートする方法です。電力事業者は、お客様がインポートしたキーに対して全責任を負います。これには、電力事業者のセキュリティ要件を満たし 256 ビットの対称暗号化キーであるランダムなソースを使用してキーマテリアルを生成すること、キーマテリアルの全体的な可用性と耐久性に対する責任を負うこと、復元目的で電力事業者が管理するシステムにキーマテリアルのコピーを保持することが含まれます。インポートされたキーは、電力事業者がコンプライアンス要件を満たせるように設計されています。これには、電力事業者のインフラストラクチャーにキーの安全なコピーを生成または維持する機能、AWS インフラストラクチャーからインポートされたキーのコピーを直接削除する機能が含まれます。

シングルテナントの FIPS 140-2 レベル 3 で検証された HSM を統制下に置く必要がある電力事業者、契約、および規制のコンプライアンス要件を満たす必要がある電力事業者は、CloudHSM を使用できます。CloudHSM では不正使用防止策が施された HSM へのシングルテナントアクセスを利用できます。HSM は米国政府により開発された暗号化モジュール向けの FIPS 140-2 レベル 3 標準に準拠しています。CIP-011-3 の要件では、シングルテナントの FIPS 140-2 レベル 3 で検証された HSM を使用することは明示的に規定されていませんが、電力事業者は独自の内部セキュリティプログラムやコンプライアンスプログラムに基づいてこのアプローチを選択できます。

CloudHSM を使用すると、電力事業者は既存の暗号化されたデータをクラウドに直接移動できます。ただし、このようなソリューションの可用性とレイテンシーは、時間の経過とともに最適とは言えなくなる場合があります。重大なリスクは、HSM が使用できなくなった、ハードウェアに障害が発生した、暗号化キーが失われたというような場合に、電力事業者の業務が停止したり、データにアクセスできなくなったりする可能性があることです。CloudHSM は既存のデータ保護ソリューションを補完する役割を果たし、電力事業者による HSM 内での暗号キー保護を可能にします。HSM は安全なキー管理に対する米国政府標準規格に適合するように設計/検証されています。

CIP-011-3 要件 1 パート 1.2 - 電子的 BCSI を保護するための管理方法

この規格では、前のセクションで概説した電子的な技術的統制に加えて、クラウドなどのオフプレミスに保管されている BES を保護するための「管理方法」の使用も認められています。
AWS では、AWS 上のデータのセキュリティを検証するうえで、さまざまな認定やセキュリティ評価手法、および類似の方法を提供しています。

AWS Artifact は無料のセルフサービスポータルで、AWS SOC レポート、FedRAMP 認定パッケージ、その他さまざまな地域やコンプライアンス分野の認定機関による AWS のセキュリティコントロールの実装と運用の有効性を検証する証明書やレポートなどの AWS 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ます。新しいレポートがリリースされると、AWS Artifact でそれらにアクセスできます。

AWS Artifact Agreements を使用すると、電力事業者は個々のアカウントの AWS との契約や、AWS Organizations 内における自社組織の一部のアカウントの AWS との契約を確認、受諾、管理することができます。AWS Artifact で入手可能な契約には、事業提携契約 (BAA) および秘密保持契約 (NDA) が含まれます。

「AWS Artifact の開始方法」ガイドは、電力事業者が AWS Artifact へのアクセスを設定する方法と、AWS との契約を確認、承認、管理する方法を理解するのに役立ちます。詳細については、「AWS Artifact に関するよくある質問」を参照してください。

AWS 法務関連ページには、AWS カスタマーアグリーメント、AWS サービスレベルアグリーメント、AWS 利用規約、プライバシー通知など、オフプレミスの BCSI を保護するための管理方法を文書化するのに役立つリソースが掲載されています。

CIP-004-7 要件 6

CIP-004-7 要件 6 は、電力事業者に文書化されたアクセス管理プログラムを実施して、BCSI への規定されたアクセスを承認、検証、取り消すことが義務付けています。具体的には、電力事業者はアクセスを提供する前に、必要に応じた BCSI への電子的アクセスを許可しなければなりません (パート 6.1)。BCSI へのアクセスを許可された個人には承認記録があり、現在の業務を遂行するために引き続きプロビジョニングされたアクセスが必要であることを少なくとも 15 か月ごとに確認しなければなりません (パート 6.2)。解約措置の発効日の翌暦日の終わりまでにその個人が電子的 BCSI にアクセスできないようにする必要があります (パート 6.3)。

CIP-004-7 要件 6 によると、この要件において BCSI へのアクセスとみなされるのは、個人が BCSI を取得して使用する両方の能力を持っているということになります。提供されたアクセスとは、「個人に BCSI へのアクセスを提供するために取られた特定の措置 (物理キーまたはアクセスカード、ユーザーアカウントと関連付けられた権利と特権、暗号化キーなど) の結果」と見なされます。これは、使用可能な形式でのデータへのアクセスではなく、ストレージロケーションへのアクセスに重点を置いていた旧バージョンの規格から大きく前進したもので、コンプライアンス要件を満たすためにクラウドストレージの使用を奨励しています。

AWS では、電力事業者は BCSI への規定されたアクセスを完全に統制できます。AWS はお客様のアカウントのコンテンツを見ることはできません。そのコンテンツに個人情報が含まれているかどうかを含め、それに関する知識もありません。詳細については、「Mitigating Unauthorized Access to Data」を参照してください。また、AWS のお客様は、AWS Well-Architected フレームワーク のセキュリティの柱で説明されている暗号化やトークン化などのさまざまな技術を使用して、コンテンツを AWS や第三者が理解できないようにすることができます。これにより、電力事業者によって許可された個人だけが BCSI を取得して使用できるようになります。

CIP-004-7 要件 6 パート 6.1.1 - 電子的 BCSI への規定された電子アクセスの承認

CIP-004-7 要件 6 パート 6.1 の大半は、電力事業者のアクセス管理ポリシーと実践に対応しています。AWS Identity and Access Management (AWS IAM) を使用すると、電力事業者はアクセスを管理してクラウドの設定と管理アクティビティを実行できます。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。

IAM を使用すると、電力事業者は AWS アカウントごとに SAML 2.0 または Microsoft Active Directory などの OIDC ID プロバイダー (IdP) を定義できます。電力事業者は、フェデレーションユーザーの属性 (コストセンター、ジョブロールなど) を IdP から AWS に移動できます。そうした属性を元にアクセス許可を実装することにより、アクセス統制が可能になります。IAM を使用すると、電力事業者はアクセス許可を 1 回定義するだけで、IdP で属性を変更すると、AWS へのアクセスを付与、取消、修正できます。

電力事業者は、アクセス管理に IAM と AWS IAM アイデンティティセンター (AWS Single Sign-On の後継) のみを使用することもできます。これらのサービスにより、ユーザー、アクセス、および廃止プロセスを一元的に管理できます。たとえば、複雑さ、長さ、有効期限などのパスワード設定制御を、IAM または IAM と統合されている既存のディレクトリサービスで管理できます。

クラウドでは、電力事業者のシステム管理者チームは、セキュアシェル (SSH) またはリモートデスクトッププロトコル (RDP) 経由で Amazon EC2 インスタンスにアクセスできます。電力事業者が 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か 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。

電力事業者の既存のオンプレミスディレクトリサービスとアクセス統制を使用して、AWS IAM アイデンティティセンター、AWS パートナーソリューション、または Amazon Cognito と統合することで、AWS 上の情報へのエンドユーザーアクセスを統制できます。Amazon Cognito は、電力事業者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、アクセス統制をサポートしています。

CIP-004-7 要件 6 パート 6.2 – 付与されたアクセス権限の検証

AWS 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、削除することができます。 IAM には、デフォルトで不正アクセスのリスクを軽減する「すべて拒否」設定が含まれています。IAM Access Analyzer は、組織全体または特定のアカウントに対してアクティベートできます。

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。この分析のために、IAM Access Analyzer は新しいリソースポリシーまたは更新を継続的に監視し、AWS サービスに付与された権限を分析します。

電力事業者は、CIP-004-7 要件 6 パート 6.2 で義務付けられている 15 か月ごとなど、設定したスケジュールでアクセス権限を確認できます。

CIP-004-7 要件 6 パート 6.3 - BCSI アクセス権限の削除

電力事業者はまた、離職日の翌暦日の終わりまでに、個人が BCSI への規定されたアクセスを使用できないようにする手順または自動メカニズムを導入する必要があります。電力事業者には、この要件を実装するためのいくつかのオプションがあります。AWS では、IAM アイデンティティセンターを使用するか、SAML 2.0 または OIDC ID プロバイダーと IAM 統合を行うことを推奨しています。そうしておくことで、電力事業者は AWS アカウントとサービスのアクセスを一元化された場所で終了できます。

電力事業者は CloudTrail レポートと API コールを使用して、電力事業者が選択した期間内に追加または削除されたユーザーに関する情報を含む、ユーザーアクセスに関するレポートを生成できます。電力事業者はレポートを離職記録と比較し、離職日の翌暦日の終わりまでに BCSI にアクセスできなくなったことを確認できます。

規模に応じたガバナンス

電力事業者は、クラウドジャーニーのどの段階でも、様々な規模の AWS 環境を管理できます。AWS でクラウドの導入を始めたばかりであっても、新しいクラウドイニシアチブを追求している最中であっても、既存のマルチアカウントの AWS 環境を管理しつつも、組み込まれたブループリントとガードレールを備えたソリューションを希望している場合でも問題ありません。

ベストプラクティスに沿ったマルチアカウントの AWS 環境を作成または管理するために、電力事業者は AWS Control Tower を使用することができます。AWS Control Tower は、大規模な AWS 環境を管理するのに役立つ規範的なガイダンスを提供します。また、AWS 環境の継続的なガバナンスのための**ガードレール**も提供します。ガードレールは、選択したポリシーに準拠しないリソースのデプロイを防止したり、規定されたリソースの不適合を検出したりすることで、ガバナンスを統制します。

AWS Control Tower は、ベースラインを確立する AWS CloudFormation、設定の変更を防ぐための AWS Organizations サービスコントロールポリシー (SCP)、不適合を継続的に検出する AWS Config ルールなど、複数のビルディングブロックを使用してガードレールを自動的に実装します。

AWS Control Tower には、マルチアカウント環境を継続的に監視するためのダッシュボードも用意されています。ダッシュボードには、アカウントで有効になっている発見的ガードレールと予防ガードレールに関するレポートが作成され、ガードレールで有効になっているポリシーに準拠していないリソースのステータスが表示されます。

電力事業者は、AWS Control Tower が提供する BCSI 環境の可視性と統制を活用できます。

監査証跡の実施とレビュー

AWS では、電力事業者がコンプライアンス文書や検証のニーズをオンデマンドで満たすのに役立つ、サービス固有のセキュリティログと監査ログを多数提供しています。AWS CloudTrail は、AWS マネジメントコンソール、AWS SDK、コマンドラインツール、AWS の他のサービスを通

じて実行したアクションを含む、AWS アカウントアクティビティのイベント履歴を提供します。これらのログには、BCSI を安全に扱うための統制が実施されていることの検証に役立つ詳細が含まれています。CloudTrail は、安全な保管と分析のために、Amazon S3 にログを配信することもできます。

Amazon S3 に BCSI を格納する電力事業者は、S3 サーバーアクセスログを有効にしてオブジェクトレベルのアクティビティと認証の失敗をキャプチャし、CloudTrail をバケットレベルのアクティビティと API コールをキャプチャするように設定する必要があります。

電力事業者は Amazon CloudWatch を使用して、AWS Lambda 関数によって処理されたリクエストをログに記録できます。電力事業者には、アプリケーションでの BCSI アクセスや管理アクティビティを記録するために、必要に応じてログステートメントをコードに挿入する責任があります。その他のシステムレベルのメトリクスについては、電力事業者は EC2 インスタンスに CloudWatch エージェントをインストールできます。

セキュリティ情報およびイベント管理 (SIEM) ソリューションをすでに使用している電力事業者は、既存のツールを使用して監査証跡を確認できます。監査証跡には、AWS パートナーネットワークを通じて AWS パートナーから入手できる SIEM ソリューションも含まれます。

さらに、電力事業者は AWS のサービスや機能を使用してログデータの分析をカスタマイズできます。たとえば、Amazon Athena は VPC フローログ、CloudTrail、CloudWatch から Amazon S3 に保管された監査証跡ログをクエリできます。電力事業者は Amazon GuardDuty と AWS Security Hub を併用して自動イベント分析を行い、これらのサービスを Amazon CloudWatch Events や Lambda と組み合わせて自動修復を行うことができます。

監査証跡の保護と保存

電力事業者は、特定の情報セキュリティ担当者のみが監査証跡にアクセスできるように、きめ細かい IAM ポリシーを使用して Amazon S3 と CloudTrail を制限する必要があります。どちらのサービスも、ログデータを保護するためのバージョニング、ライフサイクルポリシー、拒否・削除機能の使用をサポートしています。CloudTrail には、CIP-011-3 要件 1 電力事業者のサポートに役立つログファイルの整合性検証機能も用意されています。

電力事業者は、コンプライアンスモードでオブジェクトロックを適用することで Amazon S3 のログを保護できます。コンプライアンスモードでは、保護されたオブジェクトバージョンは、AWS アカウントのルートユーザーを含むユーザーが上書きしたり削除したりすることはできません。コンプライアンスモードでオブジェクトをロックすると、そのリテンションモードは変更できなくなり、保持期間を短縮することはできなくなります。コンプライアンスモードは、保持期間中にオブジェクトバージョンを上書きまたは削除できないようにするのに役立ちます。

電力事業者は、専用の AWS アカウントと Amazon S3 バケットを使用して監査証跡を保持できます。また、ライフサイクルポリシーを設定して、3 か月以上経過したデータを Amazon S3 Glacier に移行することで、さらなるコスト削減も実現可能です。Amazon S3 Glacier ストレージクラスは、パフォーマンスのニーズに合わせてミリ秒から数時間単位で取り出せるオプションを提供します。電力事業者は CloudWatch ログを Amazon S3 にエクスポートすることで、ログデータを暗号化して保護し、変更を防止または検出できます。

効率的なコンプライアンス

AWS Config には、NERC CIP BCSI に関する運用上のベストプラクティスコンフォーマンスパックが含まれており、電力事業者が共通の枠組みとパッケージモデルを使用して、ポリシー定義から監査、集約レポートまで、AWS リソースの設定コンプライアンスを効率的に管理するのに役立ちます。NERC CIP BCSI コンフォーマンスパックは、電力事業者が、CIP-004-7 要件 6 - BCSI のアクセス管理と、CIP-011-3 要件 1 - NERC CIP BCSI の情報保護プログラムに関連するセキュリティおよびガバナンス統制を監視および評価するのに役立ちます。

コンフォーマンスパックには、保管中および転送中のデータの暗号化、データ漏えいの防止など、アクセス管理のベストプラクティスとデータ保護管理の実装に役立つ 60 以上の AWS Config ルールが含まれています。電力事業者は、コンフォーマンスパックを直接実行することも、必要に応じて自身の情報保護プログラムに合わせて AWS Config ルールを追加または削除することもできます。

たとえば、データ保護をサポートするために、コンフォーマンスパックは暗号化されていないストレージボリューか一般に公開されている S3 バケットかを識別します。電力事業者は CloudWatch と Amazon Simple Notification Service (Amazon SNS) 通知を作成して、コンフォーマンスパックの統制と一致しない環境内の変化について SMS メッセージか E メールで通知を受け取ることができます。これにより、電力事業者はそれらを評価し、修正が必要かどうか判断できます。

これらのパックは、AWS Config マネージドルールまたはカスタムルールと修復アクションのリストを含む YAML テンプレートを作成することにより作成できます。各コンフォーマンスパックテンプレートでは、1 つ以上の AWS Config ルールと修復アクションを使用できます。コンフォーマンスパックにリストされている AWS Config ルールは、AWS Config マネージドルール、AWS Config カスタムルール、またはその両方である可能性があります。コンフォーマンスパックのテン

プレートは GitHub でダウンロードできます。

AWS Audit Manager を使用することで、電力事業者は AWS の使用状況を継続的に監査し、リスクとコンプライアンスの評価に役立てることができます。NERC CIP BCSI に関する運用上のベストプラクティスコンフォーマンスパックを使用している電力事業者は、これを AWS Audit Manager 評価に変換できます。
Audit Manager 評価は、統制をグループ化した**フレームワーク**に基づいています。NERC CIP BCSI に関する運用上のベストプラクティスコンフォーマンスパックを使用することで、電力事業者はそのフレームワークにおける統制の証拠を収集する評価を作成できます。評価では、電力事業者は監査の適用範囲を定義できます。これには、証拠を収集したい AWS アカウントやサービスを指定することも含まれます。

評価を作成すると、Audit Manager は継続的な証拠収集を開始します。監査の時期になったとき、または内部レビューに必要と判断された場合、電力事業者は証拠をレビューし、それを評価レポートに追加して外部監査人に共有することができます。

まとめ

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、望ましい目標のほか、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必要です。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、NERC または地域の電力事業者の監査人との協力により、よりコンプライアンスへの信頼を深めることができます。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環境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。

電力事業者には、このホワイトペーパーや後述の「参考資料」セクションで説明されているようなクラウドサービスの実装に利用できるリソースを利用することが推奨されます。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。

- Amazon Web Services、プリンシパルパートナーソリューションアーキテクト、Ranjan Banerji
- Amazon Web Services、エネルギー＆ユーティリティ業界スペシャリスト、Kristine Martz
- Amazon Web Services、シニアパートナーソリューションアーキテクト、Sean Murray
- Amazon Web Services、エネルギー＆ユーティリティ業界スペシャリスト、Maggy Powell

参考資料

詳細については、以下のリソースを参照してください。

- AWS 用語集
- AWS セキュリティリファレンスアーキテクチャ (AWS SRA)
- AWS Well-Architected フレームワーク: セキュリティの柱
- NERC CIP コンプライアンスをサポートする AWS ユーザーガイド
- 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
- コンプライアンスに関するよくある質問
- AWS 基本的なセキュリティベストプラクティスのコントロール
- 電力とユーティリティのクラウドでの本番環境までの道
- AWS クラウドセキュリティのためのユーティリティ業界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ユーティリティ業界エグゼクティブガイド
- AWS 責任共有モデル
- AWS での論理的分離
- AWS NERC CIP BCSI コンフォーマンスパック
- AWS NERC CIP BCSI リファレンスアーキテクチャ
- AWS Config NERC CIP BCSI Audit Manager 評価

ドキュメントの改訂

日付	説明
2023 年 2 月	初版発行

付録 1: AWS のサービスと NERC CIP への適合

次の表は、電力事業者が NERC CIP BCSI 要件への準拠の実装や実証を支援するために使用できる AWS サービスを示しています。電力事業者は、自社の情報保護プログラムのニーズに合わせて AWS のサービスとツールの組み合わせを選択できます。これはすべてを網羅したリストではなく、この文書のこれまでのセクションで説明したサービスと概念を説明するためのものです。

NERC CIP 規格または AWS の機能と説明	AWS のサービス、機能、リソース	お客様に関する考慮事項	AWS の責任
CIP-004-7 要件 6 BCSI のアクセス管理、承認、BCSI へのアクセス権限の検証	Amazon Cognito AWS CloudTrail AWS Directory Service AWS Directory Service for Microsoft AD AWS Identity and Access Management (IAM) AWS IAM Access Analyzer AWS IAM アイデンティティセンター	電力事業者は、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。IAM は、ユーザーやロールにきめ細かな権限を設定でき、電力事業者の現在の SAML 2.0 互換のディレクトリサービスと統合できます。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、電力事業者は既存のディレクトリサービス、AWS Directory Service、IAM、Amazon Cognito を使用できます。電力事業者は、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の許可と取り消しを行うことができます。電力事業者は IAM Identity Center を有効にして、組織全体のアクセスを一元管理できます。 AWS Directory Service for Microsoft Active Directory は AWS Managed Microsoft AD とも呼ばれ、ディレクトリ対応型ワークロードと AWS リ	デフォルトでは、AWS の担当者は BCSI を含む電力事業者のコンテンツを電子的または物理的に取得して使用することはできません。AWS では、お客様の情報をカスタマーコンテンツとアカウント情報という 2 つのカテゴリに分類しています。 カスタマーコンテンツは、お客様のアカウントに関連して AWS のサービスで処理、保管、ホストするために、お客様またはいずれかのエンドユーザーが AWS に転送したソフトウェア (マシンイメージを含む)、データ、テキスト、音声、動画、画像、ならびにお客様またはいずれかのエンドユーザーが AWS のサービスを利用して前述のコンテンツから取得した計算結果をいいます。たとえば、カスタマーコンテン

	AWS マネジメントコンソール	ソースが AWS でマネージド型の Active Directory を使用できるようにします。AWS Managed Microsoft AD は Microsoft AD 上に構築されており、既存の Active Directory からクラウドにデータを同期またはレプリケートする必要はありません。標準の Active Directory 管理ツールが使用でき、グループポリシー、Single Sign-On など組み込みの Active Directory 機能を利用できます。 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把握できます。IAM Access Analyzer は継続的に実行され、外部からのシステムへのアクセスを電力事業者に即座に通知します。 AWS CloudTrail を使用すると、アカウントのガバナンス、コンプライアンス、運用、およびリスク監査が可能になります。ユーザー、ロール、または AWS サービスによって実行されたアクションは、CloudTrail にイベントとして記録されます。	ツには、お客様またはエンドユーザーが Amazon S3 に保存するコンテンツが含まれます。カスタマーコンテンツにはアカウント情報は含まれません。カスタマーコンテンツには、リソースアイデンティティ、メタデータタグ、利用ポリシー、許可、および AWS リソースの管理に関する類似の項目に含まれる情報も含まれません。カスタマーコンテンツには、「AWS カスタマーアグリーメント」と「AWS サービス条件」が適用されます。

NERC CIP 規格または AWS の機能と説明	AWS のサービス、機能、リソース	お客様に関する考慮事項	AWS の責任
CIP-011-3 要件 1 BCSI の特定、保護、安全な取り扱いにより、機密性が損なわれるリスクを軽減する	AWS Artifact Amazon Athena AWS Certificate Manager AWS Client VPN AWS CloudHSM AWS CloudTrail Amazon CloudWatch AWS Config AWS Control Tower AWS Direct Connect Amazon DynamoDB Amazon EBS Amazon EC2 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。 電力事業者は、BCSI を含む AWS アセットにタグをデプロイできます。AWS Config を使用すると、電力事業者は関連するタグ値を持つアセットをクエリできます。 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 Elastic Block Store、Amazon Relational Database Service、Amazon DynamoDB、Amazon S3 などの AWS ストレージサービスでは、保管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統制できます。また、AWS Key Management Service (AWS KMS)、CloudHSM、またはその両方を使用して保管中のデータを暗号化できます。 電力事業者は、CloudTrail、CloudWatch、Amazon Athena などのサービスを通じて証跡を実装および監査できます。これらのログには、BCSI を安全に扱うための統制が実施されていることを示すのに役立つ詳細が記載されています。	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 の統制の有効性を実証する保証レポートを参照できます。これらのレポートは AWS Artifact にあります。

	AWS Lambda AWS Landing Zone AWS Organizations AWS PrivateLink Amazon RDS AWS Resource Groups Amazon S3 AWS SDK AWS Security Hub AWS Site-to-Site VPN AWS Tags Amazon VPC		

NERC CIP 規格または AWS の機能と説明	AWS のサービス、機能、リソース	お客様に関する考慮事項	AWS の責任
規模に応じたガバナンスと効率的なコンプライアンス CIP 統制の管理と実装をサポートする AWS サービス	AWS Audit Manager AWS CloudTrail Amazon CloudWatch AWS Config AWS Control Tower Amazon GuardDuty AWS マネジメントコンソール AWS Organizations AWS Security Hub Amazon SNS NERC CIP BCSI コンフォーマンスパックの運用のベストプラクティス	電力事業者は、「**大規模なガバナンス**」と呼ばれる、大規模なクラウドアセット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 を使うと、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が自動的に完了します。セットアップには、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たブループリントが使われます。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。 AWS Organizations は、環境の一元管理とガバナンスを支援します。AWS Organizations を使用することで、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。 電力事業者は AWS Security Hub を使用して、ア	該当なし

		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。Security Hub を使用すると、電力事業者は複数の AWS 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を 1 か所で集約、整理、優先順位付けできます。 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。Audit Manager は、証拠収集を自動化し、関係者による統制のレビューを管理するのに役立ち、比較的少ない手作業で監査準備の整ったレポートを作成できるようにします。 電力事業者は、NERC CIP BCSI コンフォーマンスパックのための AWS Config 運用のベストプラクティスを使用して、環境の継続的なガバナンスチェックを実施し、実装されているセキュリティ統制を検証できます。	

付録 2: AWS NERC CIP BCSI リファレンスアーキテクチャ

AWS は、NERC CIP 規格の対象となる電力事業者が BCSI のために安全でコンプライアンスに準拠した環境を開発および実装する際に役立つ AWS のサービスを視覚的に表現するために、俯瞰的な NERC CIP BCSI リファレンスアーキテクチャを開発しました。このドキュメントには、これまでのセクションで説明したサービスの詳細な説明が含まれています。

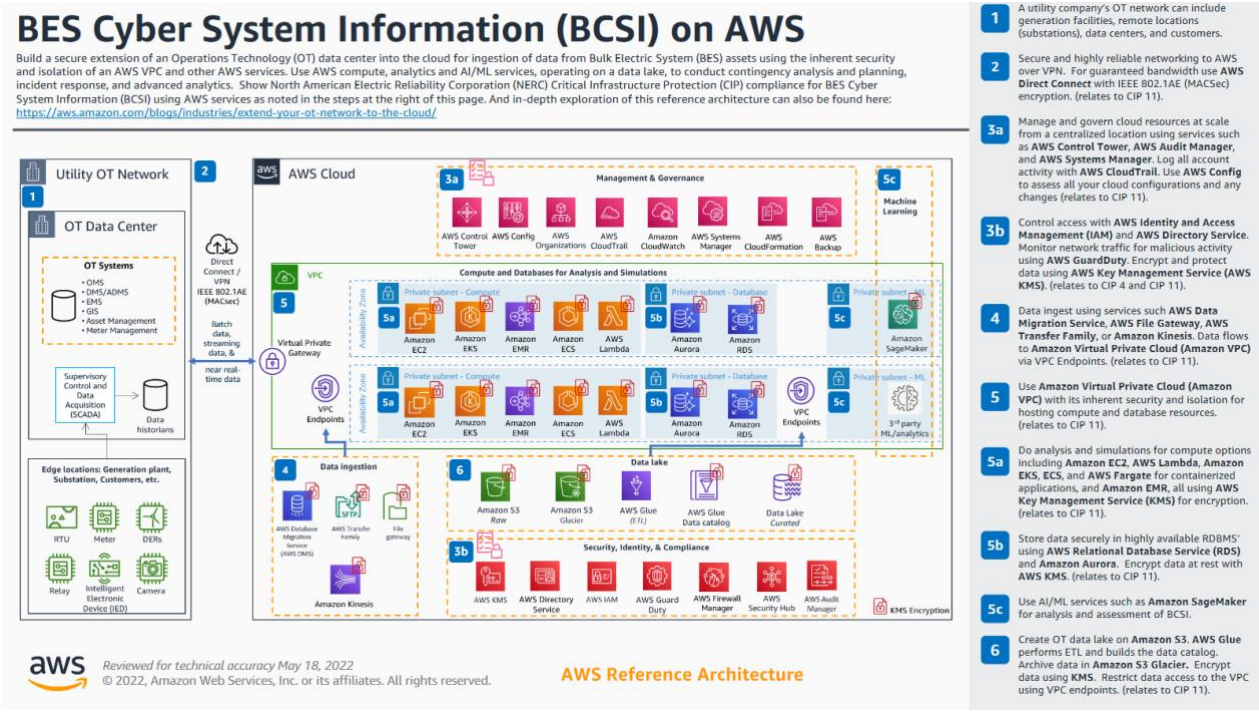

図 5: AWS NERC CIP BCSI リファレンスアーキテクチャ

以下に、リファレンスアーキテクチャに沿ったアーキテクチャ例を 2 つ示します。1 つはサーバーベースの例、もう 1 つはサーバーレスの例です。

付録 3: ユースケースの例

例 1: AWS 上のサーバーベースのアプリケーション

電力事業者は、BCSI をホストまたは使用する多くのアプリケーションを Windows または Linux サーバーで実行します。アプリケーションサーバーはデータを処理し、データベースサーバーはデータを保管します。このようなサーバーベースのシステムは、**N 層アプリケーション**と呼ばれることが多く、送電、発電、電力事業関連のその他のユースケース (資産管理、GIS、予知保全、計画および緊急時分析システムなど) に使用できます。電力事業者は、BCSI の NERC CIP 要件を順守していることを確認しながら、これらのシステムを AWS に移行できます。

その理由

AWS 上の N 層アプリケーションでは、アベイラビリティーゾーン、自動スケーリング、自動化スクリプトなどの AWS 機能を使用することで、高い耐障害性、可用性、スケーラビリティを得られ、運用労力を軽減できます。さらに、電力事業者はデータレイクを作成して分析を行うことで、データの価値を高めることができます。最新の機械学習テクノロジーを活用して、データからより深い洞察と価値を引き出すことができます。

アーキテクチャ

電力事業者は、災害発生時のダウンタイムを最小限に抑えるために、安全で可用性の高いアプリケーションを設計および構築する必要があります。AWS では、AWS KMS を使用して保管時の暗号化と TLS を使用して転送中の暗号化を行い、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デプロイすることで、これらの目的の達成を支援できます。電力事業者は、AWS Direct Connect を介して安全な VPN 接続を確立することで、AWS クラウド内のサーバーにアクセスできます。これにより、電力事業者は AWS クラウドへの専用の広帯域幅ファイバー接続が可能になります。

以下のアーキテクチャは、電力事業者が AWS のベストプラクティスと、コストを抑制しながらパフォーマンス、信頼性、セキュリティ、および優れた運用性を向上させることに重点を置いた AWS Well Architected の原則に従って、BCSI をホストするサーバーベースのアプリケーションをデプロイする方法を示しています。

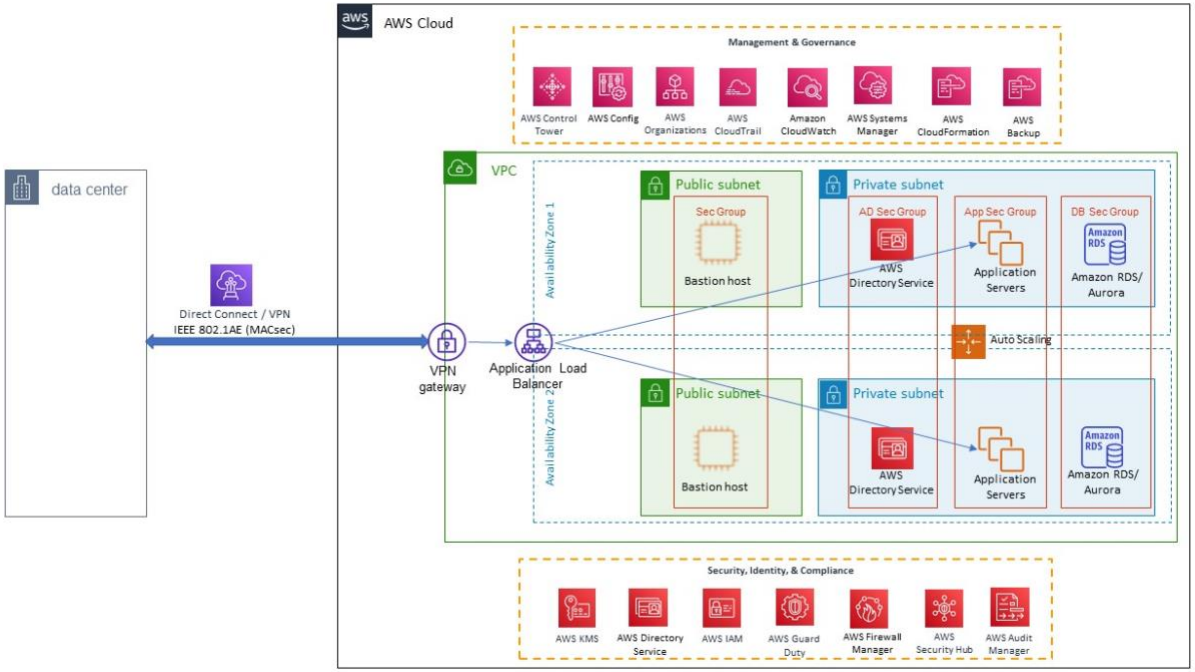

図 6: AWS アーキテクチャ上のサーバーベースのアプリケーションの例

このアーキテクチャの顕著な特徴には、次のものがあります。

1. アプリケーションはアベイラビリティーゾーン (AZ) をまたがって、Application Load Balancer の背後に配置されます。この構成により、インフラストラクチャーに障害が発生した場合でも、高い可用性とフェイルオーバーが可能になります。
2. この構成は AWS Auto Scaling を使用しているため、電力事業者は必要な最小サーバーと最大サーバーの両方を設定できるため、可用性を確保すると同時に、大規模なワークロードを処理できるようにスケールアップできます。
3. データベースサーバーは AWS RDS または AWS Aurora をマルチ AZ 構成で使用し、高い可用性とレジリエンスを実現します。
4. ストレージメディアは、AWS RDS データベース内のデータを含め、AWS KMS で暗号化されます。
5. サーバー間のコミュニケーションは、AWS Certificate Manager から発行された認証を使用して TLS を介して行われます。
6. AWS は、これらのサーバーがアクセスできる多くのサービスを提供しています。AWS PrivateLink は、サーバーと AWS サービス間のコミュニケーションをプライベートかつ暗号化するのに役立ちます。データが AWS を離れることはありません。
7. サーバーのホストに使用される AWS VPC は、IEEE 802.1AE MACsec 暗号化を使用して DirectConnect 経由で、または仮想プライベートゲートウェイを介して FIPS 準拠のアルゴリズムを使用する VPN を介して電力事業者のデータセンターに接続されます。このアーキテクチャでは、VPC はパブリックインターネットにアクセスできません。この VPC はオンプレミスデータセンターの拡張になりました。
8. NERC CIP BCSI コンフォーマンスパックテンプレートが AWS Config に適用されています。AWS Config は、暗号化されていないストレージメディアなど、データ保護から逸脱があった場合に通知します。
9. AWS 環境を継続的に監視するには、電力事業者はネットワークの異常を検出するように Amazon GuardDuty を設定する必要があります。電力事業者は、セキュリティのベストプラクティスを確実に実行できるように、AWS Security Hub の使用も検討する必要があります。
10. サーバー間のトラフィックは、セキュリティグループを使用して特定のポートに制限されます。
11. オンプレミスのデータセンターに出入りするトラフィックは、VPC のルートテーブルを使用して特定の CIDR に設定されます。

高可用性、ディザスタリカバリ、および運営の継続性

前述のアーキテクチャでは、アベイラビリティーゾーンが使用できなくなった場合でも高可用性を実現します。このアーキテクチャには次の利点があります。

1. ディザスタリカバリと事業継続のための常時稼働を実現するアクティブ-アクティブ機能。
2. 災害が発生した場合でも、フェイルオーバーや手作業は必要ありません。システムは動作を続けます。
3. システムは常に稼働していて使用中であるため、ディザスタリカバリの訓練や演習は必要ありません。
4. ほとんど使用されないインフラストラクチャーのコストを負担する必要はありません。

地域的な大災害からの保護のため、電力事業者は BCSI ワークロードを複数の AWS リージョンにデプロイすることを検討してもいいでしょう。この決定は、アプリケーションの重要度と電力事業者のリスク許容度によって異なります。詳細については、ブログ記事「How energy and utility companies can recover from ransomware and other disasters using infrastructure as code on AWS」を参照してください。

例 2: AWS のサーバーレスアプリケーション

送電事業者や発電事業者は、サーバーレスサービスを使用して AWS で取り込み、保管、処理するとよい BCSI 情報を持っている可能性があります。さまざまな組織が、BCSI の NERC CIP 要件を満たせる AWS でこれらのサービスを利用しています。AWS のサーバーレスアプリケーションは、安全性を損なうことなく、スケーラビリティ、高いレジリエンスと可用性、運用労力の軽減といった利点を活用できます。

アーキテクチャ

電力事業者は Amazon Kinesis Data Streams を使用して、運用中のテクノロジーシステムをデータソースとしてリアルタイムでデータを収集できます。収集されたデータは AWS Lambda を使用して処理され、Amazon S3 に保管されます。その後、電力事業者は Amazon Athena を使用して Amazon S3 に保管されているデータにクエリを実行し、そこから Amazon Quicksight を使用してデータを視覚化できます。このアプリケーション全体を通じて、電力事業者は保管時の暗号化に AWS KMS を使用し、転送中の暗号化には AWS Certificate Manager を使用することで、BCSI の目標を達成できます。電力事業者は、AWS クラウドへの専用の広帯域幅ファイバー接続を提供する AWS Direct Connect 経由で安全な VPN 接続を確立することで、AWS クラウド内の所有する情報にアクセスできます。

次のアーキテクチャは、電力事業者が NERC CIP コンプライアンス要件を満たしつつ BCSI 情報をホストするサーバーレスアプリケーションをどのようにデプロイできるかを示しています。

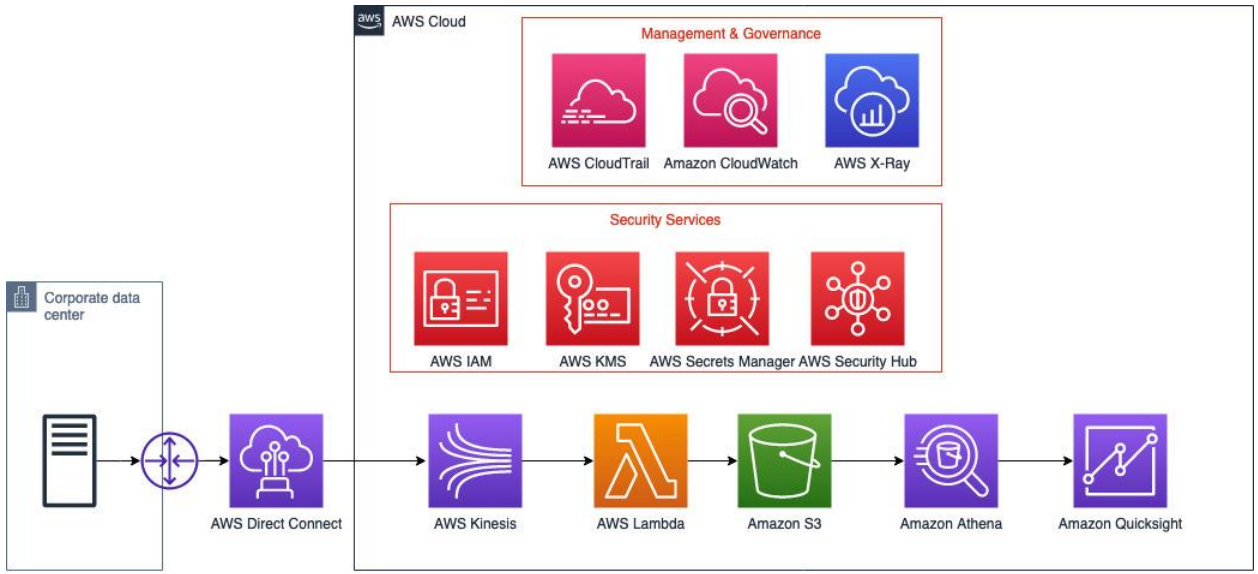

図 7: AWS アーキテクチャ上のサーバーレスアプリケーションの例

このアーキテクチャの顕著な特徴には、次のものがあります。

1. IAM は AWS サービスへのアクセスを管理するために使用されます。
2. セキュリティグループとルートテーブルは、サービス間のトラフィックを許可するように設定されています。
3. Direct Connect と IEEE 802.1AE MACsec 暗号化を使用するか、仮想プライベートゲートウェイ経由の VPN 接続を使用すると、運用中のテクノロジーネットワークと AWS サービスの間に公共のインターネット接続がないことを確実にできます。
4. AWS KMS は、データが Amazon S3 に保管されている間、保管中のデータを暗号化するために使用されます。
5. データインジェストは Amazon Kinesis Firehose を通じて行われます。
6. Lambda 関数は TLS 1.2 をサポートしています。リクエストは、IAM プリンシパルに関連付けられたアクセスキー ID とシークレットアクセスキーで署名されます。
7. Amazon S3 に保管されたデータは AWS KMS キーで暗号化されます。
8. AWS サービス間の通信はプライベートで暗号化されており、データが AWS を離れることはありません。
9. NERC CIP BCSI コンフォーマンスパックテンプレートは AWS Config を使用して適用されます。AWS Config は、暗号化されていないストレージメディアなど、データ保護から逸脱があった場合に通知します。