

HPE Aruba Networking Central

付録II: 処理の説明

<p>1. 処理の説明</p>	<p>HPE Aruba Networking Centralにより、有線、Wi-Fi、SD-WANネットワークを対象とした最新のクラウドネイティブなネットワーク運用が実現します。HPE Aruba Networking Centralは、統合されたAIベースのネットワークおよびユーザーインサイトと、IoTデバイスのプロファイリングによって安全で一貫した管理と制御を実現することで、従来の管理方法を強化します。</p>
<p>2. 処理される個人データのタイプ</p>	<p>ネットワーク管理と関連アプリケーションの一環として収集される個人データには、以下のものが含まれます。</p> <ul style="list-style-type: none"> a. デバイスMACアドレス b. デバイスIP c. デバイスのオペレーティングシステム d. デバイスのホスト名 e. ユーザー名 f. メールアドレス (ゲストが自分で登録する場合) g. 電話番号 (ゲストが自分で登録する場合) h. ソーシャルメディアのID (ゲストがソーシャルメディアのアカウントでログインする場合) i. 表示名/所属するグループ/役職 (クラウド認証を使用する場合)
<p>3. 処理される個人データのカテゴリ</p>	<p>管理者のクライアント、エンドユーザー、従業員、請負業者、臨時雇用者。</p>
<p>4. 処理の期間</p>	<p>製品によって収集、保存される情報は、ポータルへのセキュアなアクセスを確保するため、また製品の機能の実行に不可欠となる必要最小限のものです。ユーザーに関するすべてのセッションログは90日後に自動的にパージされます。</p>
<p>5. 技術的対策と組織的対策</p>	<p>処理者は、以下の付録IIIで説明するように、管理者の個人データを保護するための情報および物理的セキュリティプログラムを維持するものとします。</p>

付録III: (データのセキュリティを確保するための技術的対策と組織的対策を含む) 技術的対策と組織的対策

1. 製品のセキュリティ機能:

- a. **物理セキュリティ:** HPE Aruba Networking Centralは、包括的なセキュリティ機能およびコンプライアンス機能を提供し、最も広く利用されているIaaSプラットフォームであるAmazon Web Services (AWS) およびMicrosoft Azure上でホストされています。AWSおよびAzureでは、ネットワーク境界、インフラストラクチャ、データ、環境の各レイヤーなどの重要領域にセキュリティ対策が導入されています。
- b. **ネットワークセキュリティ:** 処理者のネットワークセキュリティは、アプリケーションとデータが存在する物理ネットワークと仮想ネットワークのセキュリティを確保します。HPEでは、IaaSプロバイダーが提供するサービスとツール、およびいくつかのサードパーティソリューションを使用して、本番環境を外部の脅威や内部の脆弱性から最大限に保護しています。処理者は、内部環境と本番環境を別個のインスタンスで実行します。内部環境は主に開発とテストに使用され、本番環境は顧客 (管理者) 専用予約されます。HPEの本番環境を他の実行中のインスタンスから物理的かつ論理的に分離することで、HPEによって最適なソフトウェア展開が顧客 (管理者) 環境で実現され、データの存在場所を常に1つの環境に限定できるようになります。
- c. **アプリケーションアーキテクチャーとセキュリティ:** Centralアプリケーションと外部との間でやり取りされるすべてのトラフィックは、SSL上のHTTPS経由で行われます。すべてのトラフィックフローはAES暗号化技術を使用して暗号化されます。Web、アプリケーション、データベースなどのさまざまなアプリケーション層が許可リストフレームワーク内で動作するように設計されています。層と層の間では、必要および必須の通信パスのみが許可されます。不正アクセスや悪意のあるアクセスを防止するため、層内の各インスタンスはファイアウォールルールによって保護されます。
- d. **データセキュリティ:** デバイスおよびユーザー間のすべてのデータ交換はHTTPSを使用して行われます。蓄積されるデータは暗号化されて保存されます。データのバックアップは定期的に行われ、バックアップデータは冗長的に保存されます。組織体制として、HPEではアプリケーションのセキュリティ面と運用面のすべてを管理するDevOpsチームを配備しています。
- e. **地理的な可用性:** HPE Aruba Networking Centralは世界中の複数の地域で利用可能であるため、管理者はアカウントを作成する地域を選択することができます。この選択に影響を及ぼす要因はさまざまです。たとえば、組織によってはすべてのデータを特定の地域に保存することを要求したり、データの処理や保存方法に規制上の制限を課したりする場合があります。

HPE Aruba Networking Centralは、選定されたAmazon Web Services (AWS) およびMicrosoft Azureのデータセンター内のクラスターに展開されており、クラウドプロバイダーがコンピューティングおよびストレージインフラストラクチャを提供しています。以下の表は、HPE Aruba Networking Centralのクラスターと対応する地域の一覧を示しています。

HPE Aruba Networking Centralのクラスター	AWSリージョン (クラスターが配置されている都市)	サインアップURL
US-1	米国西部 (オレゴン)、 us-west-2	portal.central.arubanetworks.com/signup
US-2	米国西部 (オレゴン)、 us-west-2	portal-prod2.central.arubanetworks.com/signup or console.greenlake.hpe.com
US-West-4	米国西部 (オレゴン)、 us-west-2	portal-uswest4.central.arubanetworks.com/signup
US-West-5	米国西部 (オレゴン)、 us-west-2	common.cloud.hpe.com
China-1	中国 (北京)、 cn-north-1	portal.central.arubanetworks.com.cn/signup
EU-1	EU (フランクフルト)、 eu-central-1	portal-eu.central.arubanetworks.com/signup
EU-Central2	EU (フランクフルト)、 eu-central-1	common.cloud.hpe.com
EU-Central3	EU (フランクフルト)、 eu-central-1	console.greenlake.hpe.com
Canada-1	カナダ (中央)、 ca-central-1	portal-ca.central.arubanetworks.com/signup

HPE Aruba Networking Centralのクラスター	AWSリージョン (クラスターが配置されている都市)	サインアップURL
APAC-1	アジア・太平洋地域 (ムンバイ)、 ap-south-1	portal-apac.central.arubanetworks.com/ signup
APAC-East1	アジア・太平洋地域 (東京)、 ap-northeast-1	portal-apaceast.central.arubanetworks.com/ signup
APAC-South1	アジア・太平洋地域 (シドニー)、 ap-southeast-2	console.greenlake.hpe.com

HPE Aruba Networking Centralのクラスター	Azureリージョン (クラスターが配置されている都市)	サインアップURL
UAE North1	UAE北部 (ドバイ)	common.cloud.hpe.com

管理者に割り当てられたデバイス上のすべてのアクティビティは、選択されたクラスターで処理されます。これには、HTTPS接続を通じて送信されるネットワーク統計情報やテレメトリデータが含まれます。すべての管理者アカウントの構成データも、選択されたクラスターに保持されます。

ネットワークデバイス (アクセスポイント、スイッチ、ゲートウェイ) と管理者デバイスに関連するすべてのデータ (個人データを含む)、およびその他のユーザーデータは、同じクラスター内のデータベースに保存されます。必要に応じて行われる追加の処理も、同じクラスター内のコンピューティンスタンス上で実行されるか、HPE Aruba Networking製品サービスのDPSAに従って処理されます。

— セキュリティ対策:

- 処理者は、管理者の個人データの保護を目的とする以下の情報および物理的セキュリティプログラム (「処理者セキュリティプログラム」) を維持するものとします。
- 処理者のインフラストラクチャには、適切な最新バージョンのシステムセキュリティソフトウェア (ホストファイアウォール、アンチウィルス保護、最新のパッチおよびウィルス定義など) が組み込まれています。処理者は、不正使用のパターン、不審なアクティビティ、承認されていないユーザー、その他のセキュリティリスクを監視、検出、報告する侵入検知システムを含む、インフラストラクチャに関連するイベントの記録を保持します。
- 従業員と請負業者は、処理者のプライバシーおよびセキュリティポリシーに関する研修を受けており、プライバシーおよびセキュリティ対策に関するそれぞれの責任範囲を認識しています。処理者の従業員と請負業者には、管理者の個人データの機密を保持し、管理者の個人データの処理に関して適用される処理者のポリシー、規範、または要件を遵守することが契約によって義務付けられています。これらのポリシー、標準、要件に違反した場合は調査の対象となり、処理者による解雇または契約解除まで含む、懲戒処分を科される場合があります。
- 管理者が、サービスに影響を与える個人情報漏洩のインシデントを発見した場合、管理者は速やかに処理者に対してその旨を通知し、個人情報漏洩の範囲を報告するものとします。この通知は処理者セキュリティオペレーションセンターにメール (security@hpe.com) で送信するものとします。

[HPE.com](https://www.hpe.com) にアクセス

[今すぐチャット](#)

© Copyright 2026 Hewlett Packard Enterprise Development LP. 本書の内容は、将来予告なく変更されることがあります。ヒューレット・パカード エンタープライズ製品およびサービスに対する保証については、すべて当該製品およびサービスの保証規定書に記載されています。本書のいかなる内容も、新たな保証を追加するものではありません。本書の内容につきましては万全を期しておりますが、本書中の技術的あるいは校正上の誤り、省略に対しては責任を負いかねますのでご了承ください。

AzureおよびMicrosoftは、米国および/またはその他の国におけるMicrosoft Corporationの登録商標または商標です。すべてのサードパーティの商標は、それぞれの所有者に帰属します。

a50009439JPN, Rev. 3

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

