



FARONICS™ Cloud

アーキテクチャとセキュリティの概要

はじめに

Faronics Cloudは、Faronics Cloud Deep FreezeとFaronics Cloud Deploy（以後、「Faronics Cloud」とする）に関連しています。

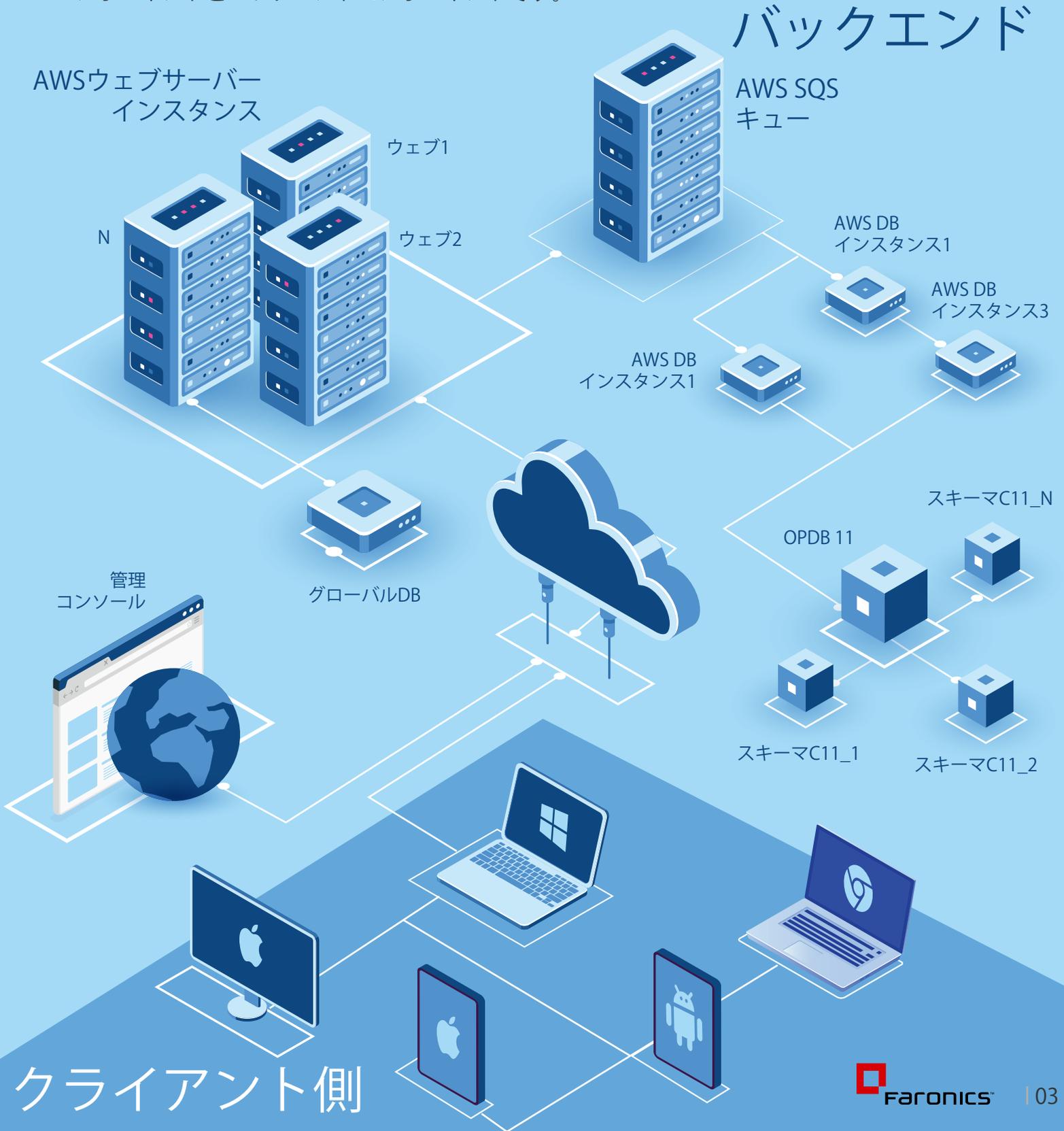
Faronics Cloudは、顧客によるインターネットを介したエンドポイント管理を簡素化することができる統合プラットフォームです。Faronics Cloudには、PC管理やMac管理、モバイルデバイス管理、アンチウイルス、アプリケーションのホワイトリスト化、データ保護、資産管理、電力管理等、幅広いサービスが含まれています。

本文書では、FaronicsのCloudアーキテクチャに関する大まかな概要を提供しています。責任共有モデルの元、どのように当事者らによって顧客データのセキュリティやプライバシーが保護されるのかについて説明されています。また、Faronics Cloudのセキュリティ責任を果たすためにFaronicsチームが従っているセキュリティポリシー、プロセス、プラクティスの概要についても説明されています。



アーキテクチャ概要

Faronics Cloudは、2つの主要なコンポーネントで構成されています：クライアント側コンポーネントとバックエンドコンポーネントです。



クライアント側コンポーネント

各マネージドコンピュータ（クライアント）には、Cloud Agentとクライアントのポリシー設定で指定された様々なサービスが含まれています。特定のサービスでは、帯域幅を節約するために顧客がオプションでローカルネットワーク内にキャッシュサーバーをセットアップすることができます。システム管理者は、インターネットブラウザを介してマネジメントコンソールにアクセスします。

バックエンドコンポーネント

Faronics CloudのバックエンドコンポーネントはAmazonウェブサービス（AWS）でホストされています。生産環境は2つのAWS領域でホストされています：US West（オレゴン）とEU（アイルランド）です。バックアップレプリカの環境は2つのAWS領域でホストされています：災害復旧用のUS East（N.バージニア）とEU（フランクフルト）です。ウェブサーバーファームは、マネージドクライアントとCloud Consoleからのすべてのクエリーを受信して応答し、AWSシンプルキューサービス（SQS）を介してデータベースサーバーへとクエリーを引き渡して処理をします。AWS Multi-AZ RDSインスタンスでホストされているグローバルデータベースには、グローバル要求されるシステムデータが格納されています。別のデータベースには、各顧客用に作成された隔離データベーススキーマが格納されています。

Faronics Cloudセキュリティ とプライバシー保護

Faronicsにとって情報セキュリティと顧客プライバシーは最重要事項となっています。業界セキュリティのベストプラクティスに従うことで、Faronicsは顧客のデータとプライバシーを偶発的/故意の抜き取り、流出、インテグリティの侵害、ハッキングから保護しています。

責任共有モデル

Cloudソリューションとして、データセキュリティの責任は、AWS（Faronics CloudのCloudサービスプロバイダ）と、Faronics（顧客へのCloudサービスプロバイダ）、Faronics Cloudの顧客で共有されています。

AWSのインフラストラクチャとサービスは複数の業界特有の標準を満たしており、以下が含まれています：



Cloudセキュリティア
ライアンス (CSA)



HIPAA



米国モーションピクチャア
ソシエーション (MPAA)



AWS のインフラストラクチャとサービス

AWSは、ホワイトペーパー、レポート、証明書、認定、その他の第三者機関による認証を通じてそのIT制御環境に関する詳細情報を提供しています。詳細情報については、次のウェブサイトにて提示されているリスクとコンプライアンスに関するホワイトペーパーを確認してください：<http://aws.amazon.com/security>。

Faronicsは、バックエンドOS、ネットワーク、ファイアウォール構成、プラットフォーム&アプリケーション管理、顧客データのセキュリティに関して責任を負います。弊社のセキュリティポリシーとプラクティスは、以下の顧客データ&プライバシー保護、及びセキュリティポリシー&プラクティスにて説明されています。

Faronics Cloudの顧客は、Faronics Cloudアカウントへのアクセスと許可を管理すること、また信用情報の安全を確保し、強力なパスワードを使用することによって独自のデータセキュリティを実現する責任があります。

顧客データ & プライバシー保護

回収された顧客データ

Faronicsは以下の理由でのみ個人情報を回収します：

- 製品とサービスを開発して管理し、顧客に提供するため
- 製品やサービスの更新、アップグレード、強化について顧客に連絡するため
- サービス期間の更新オプションの提供について直接、または再販売業者を通して顧客に連絡するため
- 興味を持ちそうな製品やserviceについて直接顧客に連絡するため
- 顧客への高水準のサービスを確保するため
- 顧客のIDを確認するため
- 法的な要求事項を満たすため

Faronics Cloudシステムでは、顧客が利用するサービスに応じて以下の顧客データを回収する場合があります：

- 顧客のIDとアカウント情報（組織名、ユーザー名、パスワード、役職、電話番号、Eメールアドレス等を含む）
- 顧客のデバイス情報（デバイス名、IPアドレス、MACアドレス、Faronics Cloudサーバーに接続した日時等を含む）
- 顧客のデバイス利用情報（ログオン/ログオフ日時、デバイスにインストールされているソフトウェア、デバイス上でのソフトウェア利用等を含む）
- Faronics Cloudサービスの構成とセレクション

顧客データのセグメント化

Faronics Cloudは顧客データ（デバイス詳細を含む、ただし個人情報は除く）を専用のデータベーススキーマにセグメント化しています。その中にあるすべての表は特定の顧客に属する形になっています。各顧客特有のデータベーススキーマは、AWSの共有データベースインスタンス上でホストされています。アーキテクチャは、顧客が専用データベースインスタンスに自身のデータを要求することができるのに十分な柔軟性を持っています。データを分離する際に顧客に対して追加の費用が請求される場合がありますのでご注意ください。

転送中の顧客データに対する保護

Faronics Cloudサーバーは、HTTPS (TLS 1.2) 暗号化を使用しています。Faronicsは、保存中の機密顧客データ（パスワード、ポリシー、データベース接続ストリング等）をデータの種別に応じて暗号化します：

- パスワードハッシュでは、片方向暗号化を使用します。
- データベース接続ストリングは、256ビットのRijndaelアルゴリズムを使用して暗号化されます。
- ポリシーは、Microsoftベースの暗号化サービスプロバイダがサポートするRC4ストリーム暗号化アルゴリズムを使用し、特定のサービスに応じて暗号化されています。

ストレージ内の顧客データに対する保護

Faronics Cloudバックアップデータは暗号化を有効にした状態でAWSに格納されています。機密データはいつも事前に暗号化されています。



セキュリティポリシー&プラクティス

開発& QAセキュリティポリシーとプラクティス

Faronicsの開発とQAプロセスは、セキュリティリスクと脆弱性を意識して設計されています。

関連するベストプラクティスには、以下が含まれます（これに限らず）：

- ソースコードのビルドはマルウェア対策でスキャンされ、セキュリティコードはデプロイ前にレビューされます。
- 開発チームはアプリケーションレベルのペネトレーションテストを業界のベストプラクティスとガイダンスの記載に従って定期的に行います。
- オペレーションチームは、異なる損失シナリオに対して定められたテストスケジュールごとにクリティカルサービスのビジネス継続性とディザスタリカバリ計画をテストします。
- セキュリティテストは、デプロイ前にすべてのリリースに対して実行されます。
- システム/ソフトウェア開発ライフサイクル (SDLC) 内で、「侵害の防止」と「侵害の想定」の両方のセキュリティ体制を使用してセキュリティを継続的に改善していきます。

Faronicsは、大きな変更の実装を制御するためにソフトウェア開発及びリリース管理プロセスを確立しました。それには以下が含まれます：

- 予定されている変更は特定され、文書化されます（フィーチャー仕様の作成やコンポーネントデザインを含む）
- 製品事業目標、優先順位、シナリオは製品計画の段階で特定されます
- 事前に定義された基準に基づいて運用準備がレビューされ、全体のリスクとインパクトが評価されます
- 試験、承認、及び変更管理は、DEV（開発）、INT（統合試験）、STAGE（プリプロダクション）、PROD（製造）の環境に関する開始基準と終了基準に基づいて適切に定められています
- Faronicsは、以下のベストプラクティスを使用してデータベース入力及びユーザー入力のサニタイズを図っています：
 - 入力は、基本認証と.NET SqlCommand、SqlParameterの使用の適切な回避によって制限されています
 - SQLクエリーが直接操作または結合されることはありません

運用のセキュリティポリシー&プラクティス

以下の業界セキュリティのベストプラクティスに従うことで、Faronics Cloudの運用は顧客データに対して強固な保護とプライバシーを提供するようにデザインされています。関連するポリシーには、以下が含まれます（これに限らず）：

- AWS IAM（ID、アクセス管理）サービスが、バックエンド環境におけるユーザー、グループ、ロールの認証管理に使用されています。
- AWS VPC（バーチャルプライベートCloud）、Network ACL（アクセス制御リスト）、及びセキュリティグループがバックエンドインフラストラクチャ（EC2インスタンス、RDSインスタンス）を保護するために使用されています。
- AWSプラットフォーム上のアクティビティはAWS CloudTrailを使用して監査されています。
- Faronics Cloud製造サイトへの変更は、変更管理文書のガイドラインに準拠した形で行われます。
- コンポーネントとプロセスは、ユーザーが業務を遂行するために最低限必要な権限を用いて提供されています。
- Faronics Cloudサービス内の顧客データへのアクセス権を持つFaronicsの内部承認済みスタッフは、MFA（マルチファクタ認証）ログインを使用することが求められています。
- システムインフラストラクチャは、冗長性とスムーズな不具合時のハンドリングを意識して構成されています。

- データは定期的にバックアップされており、災害発生時のリカバリ目的でバックアップデータは定期的に確認されています。バックアップの標準、ポリシー、プロシージャー、制御は認証され、文書化されています。
- Cloudサービスは、データセンターの停電、ネットワーク不良、その他の災害発生状況において、同一AWS領域内の異なるアベイラビリティゾーン、または異なるAWS領域に格納することができます。復元プロセスは、定義及び文書化されています。
- 運用は、定期的な内部セキュリティ監査の対象で、システム管理者やその他のパーティーが日常の運用で実行している内容のトレース、ログ、その他の情報を元に行われます。

参照と詳細

[AWSセキュリティのベストプラクティス \(Amazonウェブサービスによる\)](#)

[Cloudコンピューティングプラスに対する信用できない脅威トップ12：業界インサイト \(Cloudセキュリティアライアンス \(CA\) による\)](#)

[OWASPトップ10 2017 - ウェブアプリケーションセキュリティの重大リスク トップ10](#)

注意：本文書は、情報提供の目的でのみ提供されています。本書発行時点におけるFaronicsの製品オファーとプラクティスを表しており、事前の通知なく内容が変更される場合があります。本文書内の情報、及びFaronics製品/サービスの使用については、顧客が個別に判断する責任があり、当該製品/サービスは「現状のまま」提供されており、明示的または黙示的に関わらずいかなる保証もされていません。本文書は、Faronics、その関連会社、サプライヤー、またはライセンサーからのいかなる保証、宣言、契約的コミットメント、条件、約束を形成するものではありません。顧客に対するFaronicsの責任及び法的責任は、Faronics契約書によって管理されています。本文書は、Faronicsと顧客間の契約の一部ではなく、またこれによって契約内容が変更されることもありません。



現在のコンピュータ環境でFaronicsソリューションの利点を活用する方法については、www.faronics.comを参照してください

米国

5506 Sunol Blvd, Suite 202
Pleasanton, CA, 94566 USA

フリーダイヤル：1-800-943-6422
ファックスフリーダイヤル：
1-800-943-6488

sales@faronics.com

ヨーロッパ

8 The Courtyard, Eastern Road,
Bracknell, Berkshire
RG12 2XB, United Kingdom

電話番号：+44 (0) 1344 206 414

eurosales@faronics.com

カナダ/国際

609 Granville Street, Suite 1400
P.O. Box 10362, Pacific Centre
Vancouver, BC, V7Y 1G5

電話番号：+1-604-637-3333
ファックス：+1-604-637-8188

sales@faronics.com

シンガポール

6 Marina Boulevard
#36-22 The Sail At Marina Bay
Singapore, 018985

電話番号：+65 6509 4993
ファックス：+65 6722 8634

sales@faronics.com.sg