ビル向けクラウドサービス
情報セキュリティ対策
第 1 版

アズビル株式会社

グループクラウドサービス部

Ver	発行日	内容
1.0	2024 年 6 月 28 日	初版発行

目次

1. はじめに

1.1. 説明資料の目的

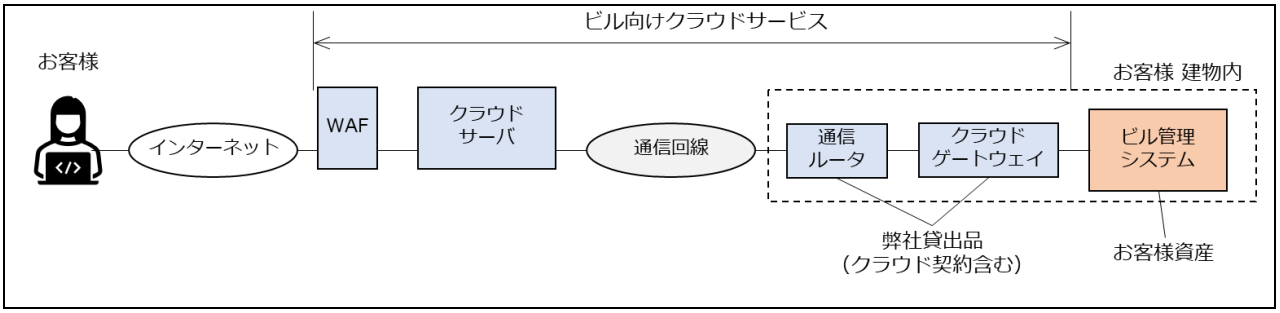
ビル向けクラウドサービスを、お客様が安心してご利用いただくため、当サービスの情報セキュリティ対策を全体的に説明し、ご理解いただくための資料です。

1.2. サービス概要

ビル向けクラウドサービスは、建物利用者や建物管理者が、インターネット経由で建物専用 Web サイトにアクセスし、中央監視装置で管理する空調運転スケジュールの予約や機器操作したり、建物のエネルギー分析や、保全業務の情報管理を行うシステムです。

1.3. システム構成

ビル向けクラウドサービスのシステム構成は、お客様向けに提供する本番環境に加えて、開発環境（新機能や改善の開発を行うための環境）、試験環境（開発が完了後にテストする環境）が含まれます。これにより、各フェーズでの変更やテストが本番環境に影響を与えることなく行うことが可能です。



ビル管理システム	建物設備を監視制御するシステム（別名 中央監視システム、BAS）
クラウドゲートウェイ	クラウドサーバからビル管理システムへの通信の中継およびビル管理システムからのデータ収集のために設置
通信ルータ	クラウドサーバと通信回線接続のための装置（モバイル型、光回線型）
通信回線	通信キャリアの閉域型ネットワーク　モバイル型または光回線型案件毎に対応
クラウドサーバ	クラウドアプリケーションやデータベースなどのクラウドプラットフォーム全体（クラウドプラットフォーム事業者のクラウドプラットフォームを利用）
WAF	Web アプリケーションファイヤーウォール（インターネット経由で、外部からの Web アプリケーションの脆弱性を突いた攻撃へ対するセキュリティ対策するための装置。WAF 事業者のサービスを利用）

2. 情報セキュリティの重要性

2.1. 情報セキュリティの基本概念

情報セキュリティは、情報の機密性、完全性、可用性を確保するための一連の対策やプロセスを指します。これらの概念は、情報が適切に保護され、信頼性を維持するための基礎となります。

- **機密性（Confidentiality）:** 情報の機密性は、情報が不正に取得されるリスクを最小限に抑え、特定の情報が許可された個人やシステムにのみアクセスできる状態のことです。具体的な施策として、データ暗号化やアクセス制御リスト（ACL）の設定があります。
- **完全性（Integrity）:** 情報の完全性は、情報の改ざんや破損を防ぎ、正確な情報が保持できる状態のことです。具体的な施策として、デジタル署名 やチェックサムを使用があります。
- **可用性（Availability）:** 情報の可用性は、システムのダウンタイムを最小限に抑え、サービスの継続性を確保し、必要なときに情報にアクセスできる状態のことです。具体的な施策として、冗長化、バックアップ、およびディザスタリカバリ計画があります。

2.2. クラウド環境におけるリスクと脅威

クラウドサービスにおけるリスクと、リスクに対して適切な対策を実施しています。

- **データ漏洩:** データが不正アクセスや内部不正で漏洩するリスクがあります。これを防ぐために、データの暗号化、厳格なアクセス制御、監査ログを活用しています。
- **アカウントの乗っ取り:** クラウドアカウントが不正取得されると、データの不正取得や改ざん、削除のリスクがあり、これを防ぐため、強力なパスワードポリシーと異常なログイン監視を実施しています。
- **サービスの中断:** DDoS 攻撃やビル向けクラウドサービスのシステムが稼働するプロバイダーのシステム障害でサービスが中断されるリスクがあります。これを防ぐために、WAF の導入や障害監視を行っています。
- **マルチテナント環境の脆弱性:** 複数のお客様が同じインフラを共有するため、一つの脆弱性が他に影響するリスクがあります。これを防ぐため、お客様ごとのデータを物理的に分離しています。
- **データ消失:** 災害やサーバー障害、不正アクセス、設定不具合でデータが消失するリスクがあります。これに備え、定期的にデータをバックアップしています。

3. セキュリティ方針とガバナンス

3.1. セキュリティポリシーの概要

情報セキュリティを最優先事項として位置づけ、セキュリティポリシーは、情報の機密性、完全性、可用性を確保するために策定し、全社員がこれに従うことを義務付けています。

セキュリティポリシーは定期的に見直し、最新の脅威やリスクに対応するために更新しています。全社員は定期的なセキュリティトレーニングを受け、ポリシーの遵守を徹底しています。

当社の情報セキュリティ基本方針は、ホームページに公開しております。

azbil グループ情報セキュリティ基本方針

https://www.azbil.com/jp/corporate/vision/information-technoroly/index.html

3.2. ガバナンス体制と責任者

クラウドサービスの情報セキュリティガバナンス体制の主な構成要素と責任は下記の通りです。

- **経営情報セキュリティ責任者:**事業および社内における情報セキュリティ戦略、実行・監督に関する経営責任者。
- **情報セキュリティ専門部門（CSO）:**事業および社内におけるセキュリティ戦略を策定し、実行、監督する専門部署します（弊社部署名　サイバーセキュリティ室）。
- **クラウド運用部門:**クラウドサービスにおけるセキュリティ運用を含む業務運用およびIT運用の戦略を策定し、実行、監督します（弊社部署名　サービス本部グループクラウドサービス部）。
- **情報セキュリティのための方針群**:クラウドサービスは、azbil グループ情報セキュリティ基本方針、及びクラウドサービスの情報セキュリティ方針に従い、運用しています。
- **情報セキュリティの役割及び責任**: クラウドサービス利用契約書、クラウドサービス利用契約約款及び仕様書などにて契約やサービスの内容を定義し、サービスを提供しています。
- **関係当局との連絡**: グループクラウドサービス部の所在地は、神奈川県藤沢市川名 1-12-2 です。クラウドサービスで保存いただくデータの所在は、日本国内です。
- **クラウドコンピューティング環境における役割及び責任の共有及び分担**:弊社のクラウドサービス提供者としての役割、システムが稼働するプロバイダー事業者、及びビル向けクラウドクラウドサービスを利用するお客様の間で、情報セキュリティの役割と責任を分担します。

4. 認証とアクセス管理

4.1. ユーザー認証方法

ユーザー認証を強化するためにパスワード認証を採用しています。

- **パスワード認証:** ユーザーはサービスにアクセスする際にパスワードを入力する必要があります。当社は強力なパスワードポリシーを採用しており、最低限の文字数、特殊文字の使用、定期的なパスワード変更を推奨しています。

4.2. アクセス権限管理

ユーザーのアクセス権限を厳密に管理するために、ロールベースのアクセス制御を採用しています。

- **ロール定義:** 各業務に必要な権限を持つロールを事前に定義します。例えば、お客様に対しては一般ユーザーロール、管理者ロール、弊社内に対しては管理者ロール、開発者ロール、閲覧専用ロールなどがあります。
- **最小権限の原則:** ユーザーには、その業務を遂行するために必要な最小限の権限のみを付与します。これにより、不必要な権限を持つことで発生するリスクを軽減します。
- **定期的な権限レビュー:** ユーザーのアクセス権限は定期的に見直され、不要な権限が付与されていないか確認します。また、社員の異動や退職時には直ちに権限の変更や削除を行います。

4.3. ログイン試行の監視とアラート

ユーザーのログイン試行（認証情報を入力してログインを試みる行為)を常に監視し、異常な活動が検出された場合には即座にアラートを発するシステムを導入しています。

- **ログイン試行の監視:** すべてのログイン試行はリアルタイムで監視され、異常な活動（例：短時間での連続したログイン失敗、通常と異なる IP アドレスからのアクセスなど）が検出されると記録します。
- **アラートシステム:** 異常なログイン試行が検出された場合、即座にアラートが発せられます。このアラートは管理者に通知され、迅速な対応が可能となります。
- **アカウントロック:** 一定回数のログイン失敗が続いた場合、アカウントは自動的にロックされます。これにより、総当たり攻撃などを防止します。

- **ログの保存と分析:** すべてのログイン試行とアラートは詳細に記録され、定期的に分析されます。これにより、潜在的な脅威を早期に発見し、対策を講じることができます。

4.4. 特権的ユーザーのログ管理

特権的ユーザーの操作はシステムに重大な影響を及ぼす可能性があるため、厳密なログ管理が求められます。当社では、特権的ユーザーの操作ログを詳細に記録し、定期的な監査を実施しています。

- **操作ログの記録:** 特権的ユーザーの全ての操作は、詳細なログとして記録されます。これには、ログイン、ログアウト、設定変更、データ操作などが含まれます。

4.5. 利用環境管理

- **利用者の秘密認証情報の管理**: お客様に提供する管理ツール等を使い、お客様の管理者はビル向けクラウドサービスを利用するユーザーの秘密認証情報の初期設定や変更ができます。
- **仮想コンピューティング環境における分離**: マルチテナント環境で動作しますが、ユーザーID によるアクセス資源の分離を実施し、別テナントへの不正アクセスを抑止しています。
- **仮想マシンの要塞化**:要塞化（例えば必要なポート、プロトコル及びサービスだけを有効とする）及び利用する各仮想マシンへ適切な手段（例えばマルウェア対策、ログ取得）の実施を行っています。
- **特権的アクセス権の管理**: 弊社内における特権的アクセス権の管理はログイン ID とパスワードによる認証に加えて IP アドレス制限をしています。

5. データ保護

5.1. データ暗号化(転送時)

転送時のデータを暗号化することで、顧客の情報が不正にアクセスされるリスクを最小限に抑えます。

- **転送時のデータ暗号化**: データがクラウドとユーザー間で転送される際には、SSL/TLS（Secure Sockets Layer/Transport Layer Security）プロトコルを使用して暗号化されます。これにより、データがネットワーク上で盗聴されるリスクを防ぎます。

5.2. データバックアップとリカバリ

データバックアップとリカバリはクラウドサービスの可用性とデータの完全性を確保するために不可欠です。

- **データバックアップ**: データは定期的にバックアップされ、複数の地理的に分散されたデータセンターに保存されます。これにより、災害やシステム障害が発生した場合でもデータの可用性を確保します。バックアップは毎日行われ、リカバリ作業に十分なデータを保存します。
- **リカバリ手順**: データが失われた場合や破損した場合には、迅速にリカバリを行うための手順を整備しています。

5.3. データ消去

契約終了した際には、適切な方法でデータを消去することが重要です。

- **データ消去**: 中間処理などで生じたデータなどは不要になった時点で、データ消去します。
- **クラウドサービス利用者の資産の除去**: お客様がサービス契約を解約した場合、お客様がクラウドサービス上に作成・保存した情報資産(保存データ)は弊社のデータ消去手順に従ってデータ及び保管媒体を消去します。解約時点でお客様がクラウド上のデータの取り出しを必要とされる場合は、お客様からの申し入れに基づき、弊社から提供します。

6. ネットワークセキュリティ

6.1. ファイアウォール・WAF・侵入検知システム

外部からの不正アクセスや攻撃を防ぐため当社では、以下のような対策を実施しています。

- **ファイアウォール**:複数層のファイアウォールで保護しており、ネットワークトラフィックを監視し、不正なアクセスをブロックします。
- **WAF（Web アプリケーションファイヤーウォール）**: WEB アプリケーションの脆弱性に対して有効な WAF を採用しています。SQL インジェクションや XSS などの攻撃から保護し、DDoS 防御、悪意のあるボット検知や管理、リアルタイム監視、不正アクセスを監視しています。
- **侵入検知システム**: 悪意のある IP アドレスやドメインのリスト、機械学習 モデルなどを使用して、システム内の予期しないアクティビティ、悪意のあるアクティビティを特定しています。
- **ネットワークの分離**:ネットワーク間の領域の分離を、適切に行なうため、システムを提供するネットワークとデータを保管するネットワークは分離しています。

6.2. 安全な通信プロトコル

- **安全な通信プロトコル**: TLS（Transport Layer Security）プロトコルを使用し、データを暗号化し、サーバーとクライアント間の通信の機密性と整合性を確保します。また、最新の TLS バージョンを使用し、弱点となる古いバージョンや暗号スイート（暗号組み合わせ）を無効にしています。

6.3. DDoS 対策

DDoS 攻撃（分散型サービス拒否）に対して WAF による多層防御策を実施しています。

- **トラフィックフィルタリング**:トラフィックフィルタリング技術を使用し、DDoS 攻撃の兆候を検出します。攻撃を検出した場合、自動フィルタリングし、正常なトラフィックが影響を受けないようにします。
- **スケーラブルなインフラストラクチャ**:スケーラブルなインフラストラクチャを採用し、DDoS 攻撃にも耐えられる能力を持っています。トラフィックの急増に対応し、サービスの可用性を確保します。

6.4. 建物接続用ネットワークでのセキュリティ対策

- 外部からアクセスを受けるサイトとは物理的に分離された建物側と接続すると為のネットワークを別途構成しています（インターネットとは接続しない、クローズドな専用のネットワークを形成）。
- 建物と接続するネットワークは、アズビル側でセキュリティが担保できるように設計・運用を行っております。

7. 物理的セキュリティ

7.1. クラウドプラットフォームの物理的セキュリティ

- ビル向けクラウドサービスにおけるデータベースやアプリケーションなどのシステムは、クラウドプラットフォーム事業者のサービスを利用しており、弊社は物理的なシステムを直接管理していません。

7.2. 通信ネットワークの物理的セキュリティ

- お客様建物と弊社センター（クラウドプラットフォーム）との間を結ぶ通信ネットワークは、大手の通信事業者のネットワークを利用し、弊社では物理的な通信ネットワークを直接管理していません。

7.3. お客様建物内に設置した機器の物理的セキュリティ

- ビル向けクラウドサービスのため、お客様のビル管理システムと、お客様建物内で、ゲートウェイ装置および通信ルータを設置しています。
- ゲートウェイ装置および通信ルータは、弊社クラウド部門（グループクラウドサービス部の専門スタッフ）限定でID・PW管理し、それらの機器を設置する弊社サービスエンジニアに ID・PW を公開しておりません。
- ゲートウェイ装置および通信ルータは、お客様と設置場所を確認の上、お客様ビル内で外部から侵入できない場所に設置させていただきます。

8. 運用管理と監視

監視体制、定期的なセキュリティ評価と監査に関する具体的な対策について説明します。

8.1. セキュリティインシデント対応

セキュリティインシデントは、クラウドサービスの運用において避けられないリスクの一つであり、セキュリティインシデントに迅速かつ効果的に対応するための包括的なプロセスを構築しています。

8.2. 監視体制

当社のクラウドサービスでは、セキュリティとサービス運用の監視を 24 時間 365 日体制で行っています。この監視体制により、異常や潜在的な脅威を早期に検出し、迅速に対応することが可能です。

- **グループクラウドサービス部（CSD）**:ネットワークトラフィック、システムログ、セキュリティアラートを監視し、異常が検出された場合に直ちに分析と対応を行います。
- **自動化監視ツール**: 高度な監視ツールを導入しており、リアルタイムでシステムの健全性を監視しています。
- **定期的なレポート**: 監視結果は定期的にレポートとしてまとめられ、経営層および関係部門に共有されます。
- **変更管理**: お客様に通知する必要のある弊社が提供するクラウドサービスの仕様変更や仕様追加などについて、お客様へ連絡します
- **容量・能力の管理**: 弊社が契約しているクラウドサービスプロバイダ提供のクラウド環境（弊社のクラウドサービスを提供する基盤となる）上の資源について、容量・能力（ディスク使用率、メモリ使用率、CPU 使用率）を監視し、逼迫している際は資源を拡張します。。
- **実務管理者の運用セキュリティ**: お客様の管理者向けに提供する管理ツール等の取扱説明書と共に、QA サポートも提供します。

8.3. 定期的なセキュリティ評価と監査

セキュリティ対策の有効性を維持するためには、定期的な評価と監査通じて継続的な改善を図っています。

- **セキュリティ評価**: 定期的にセキュリティ評価を実施し、システムの脆弱性やリスクを特定します。。これらの結果を基に、必要な修正や対策を講じます。
- **内部監査**: セキュリティ対策の実施状況を確認するために、内部監査を定期的に実施します。監査は、セキュリティポリシーや手順が適切に遵守されているかを確認し、改善点を特定します。
- **第三者監査**: 外部の専門機関による第三者監査も定期的に受けています。客観的な視点からセキュリティ対策の有効性を評価し、ISO 27001 および ISO27017）の維持を行います。
- **技術的ぜい弱性の管理**: 弊社は、技術的ぜい弱性の情報を、常時収集しています。クラウドサービス側の対応が必要となった場合は、弊社が定期または緊急メンテナンスを実施し、セキュリティを確保します。

9. コンプライアンスと法令遵守

9.1. 情報セキュリティ認証（ISO 27001、ISO27017）

安全性を最優先に考え、セキュリティ管理体制を厳格に行なうため、下記の認証を取得しています。

- **ISO 27001:**ISO27001 認証は、情報セキュリティ管理の国際標準規格であり、。この認証を取得することで、当社のクラウドサービスが高いセキュリティ基準を満たしていることを証明し、お客様のデータ保護に対する信頼性を強化します。
- **ISO 27017:**クラウドサービスに特化した ISO27017 認証も取得しており、クラウド環境における独自のリスクに対する適切な対策が講じられていることが保証され、お客様に安全で安心なクラウドサービスを提供できることを示しています。

9.2. 法令遵守のための取り組み

情報セキュリティおよびデータ保護に関する法令や規制を遵守するために、以下の取り組みを行っています。

- **法令遵守プロセスの整備**: 情報セキュリティおよびデータ保護に関する最新の法令や規制を常に把握し、それに基づいて内部プロセスを整備しています。
- **クラウドサービス利用契約の締結**: お客様との間でクラウドサービス利用契約を締結し、データの取り扱いに関する責任と義務を明確にし、データ主体の権利を保護し、法令遵守を徹底しています。
- **証拠の収集**: 裁判所からの開示請求など、法律に基づいた正当な開示請求が行われた場合、クラウドコンピューティング環境内で生成される，デジタル証拠となり得る情報及びその他の情報について、お客様の同意を得ずにこれらの情報を提供する場合があります。
- **記録の保護**: 本クラウドサービスは、クラウドサービスの維持管理に必要となる適切なお客様のアクセス履歴、及びお客様の閲覧履歴を収集、保持しています。

9.3. プライバシーポリシー

お客様の個人情報をどのように収集、使用、保護するかを明確に説明しています。

- **個人情報の収集**: お客様から提供された個人情報を、サービス提供のために必要な範囲で収集します。収集する情報には、氏名、連絡先情報、利用履歴などが含まれます。
- **個人情報の利用**: 収集した個人情報は、サービスの提供、品質向上、セキュリティ確保、マーケティング活動のために利用されます。お客様の同意なしに、第三者に個人情報を提供することはありません。
- **個人情報の保護**: 収集した個人情報を保護するために、適切な技術的および組織的な対策として、データの暗号化、アクセス制御、定期的なセキュリティ評価などを実施します。
- **個人情報の開示、訂正、削除**: お客様は、自身の個人情報について開示、訂正、削除を要求する権利があります。当社は、これらの要求に迅速に対応します。

10. 教育とトレーニング

10.1. 社員教育プログラム

情報セキュリティの維持と強化を目的として、体系的な社員教育プログラムを実施しています。

- **アズビルグループ情報セキュリティ教育**: アズビルグループ全社員を対象に、定期的に e ラーニングにて情報セキュリティ教育を行っています。安心・安全な製品・サービスをお客様に提供し続けるために、日々変化していく脅威・リスクから azbil グループを守るために必要な情報セキュリティに関する知識を身に付けることを目的としています。
- サービスに従事する社員の情報セキュリティ教育：情報セキュリティ要件の周知徹底とクラウドサービスの運営ルール徹底を目的として、サービスに従事する要員を対象とした教育・訓練及び意識向上の策を実施しています。
- **標的型攻撃メール訓練**:全社員に対し、e ラーニング等での学習資料にて理解するだけでなく、現物メール同様の訓練を行うことで、「その時何が起こるか」を全員が理解すること、初動対応/インシデント対応を理解すること、訓練実施による課題を確認することを目的としています。
- **インシデント対応訓練**:クラウド運営スタッフに対し、インシデント発生を想定した訓練を実施しています。意識の向上、対応能力強化、対応手順の確認、課題の確認・改善を目的としています。
- **協力会社社員の教育**: 社員だけではなく、お客様建物の自動制御システム機器保守点検契約先で作業する協力会社（弊社呼称 認定サービス会社）の社員に対して、情報セキュリティ入場者教育や保守現場で使用する情報機器の台帳管理、棚卸を定期的に実施しています。

10.2. セキュリティ意識向上のための取り組み

社員一人ひとりの意識向上が不可欠であり、セキュリティ意識を高めるための取り組みを行っています。

- **アズビルグループ情報セキュリティの日の制定**: ２月２日と８月１日の年2回「azbil グループ情報セキュリティの日」を制定し、啓発活動（施策）を実施しています。アズビルグループの社員に情報セキュリティについてより一層理解を深め、高い意識を維持していくことを目的にしています。
- **アズビルグループ情報セキュリティ自己点検の実施**：部門単位、個人単位で、「自己点検」の実施による部内のセキュリティ状況の確認と是正を行います。

以上