AOULU CLOUD

セキュリティ ホワイトペーパー

アオウル株式会社

目次

AOULU CLOUD
セキュリティ ホワイトペーパー
    目次
1 はじめに
2 セキュリティ対策
    2-1 不正アクセス対策
        2-1-1 ネットワーク
            2-1-1-1 ファイアウォール
            2-1-1-2 IPS
            2-1-1-3 WAF
        2-1-2 サーバ
            2-1-2-1 ウイルス対策
            2-1-2-2 不要なサービスの停止
        2-1-3 アプリケーション
            2-1-3-1 セキュアコーディング
        2-1-4 脆弱性対策
            2-1-4-1 パッチ適用
            2-1-4-2 脆弱性診断
    2-2 暗号化
        2-2-1 CRYPTREC 暗号リスト
        2-2-2 通信内容
            2-2-2-1 TLS1.2 未満の通信無効化
        2-2-3 データ
            2-2-3-1 機密情報の暗号化
        2-2-4 ハードディスク
            2-2-4-1 ストレージシステム
    2-3 物理的セキュリティ
        2-3-1 データセンター
    2-4 ユーザー側管理機能
        2-4-1 権限設定
    2-5 セキュリティ強化オプション
        2-5-1 パスワード有効期限
        2-5-2 セッションタイムアウト
        2-5-3 アカウントロック
        2-5-4 IP アドレス制限
        2-5-5 2要素認証/2段階認証
    2-6 パスワードポリシー
    2-7 時刻同期
3 運用体制
    3-1 監視
        3-1-1 24時間365日
        3-1-2 有人監視
        3-1-3 監視内容（死活監視、リソース）、監視間隔
    3-2 運用環境
        3-2-1 専用 PC

- 3-2-2 権限管理
- 3-3 ログの取得について
- 3-4 特権 ID について
- 3-5 CSIRT の設置
- 3-6 監査
  - 3-6-1 システムアカウント
  - 3-6-2 ログ
- 4 災害対策/障害対策
  - 4-1 データセンター
  - 4-2 障害対策
    - 4-2-1 リソース拡張
    - 4-2-2 対応フローの整備
  - 4-3 データバックアップ
    - 4-3-1 取得種別
    - 4-3-2 取得間隔
    - 4-3-3 保持期間
    - 4-3-4 遠隔地保存
- 5 コンプライアンス
  - 5-1 認証
    - 5-1-1 クラウドサービス認定
    - 5-1-2 情報開示認定
  - 5-2 当社の地理的所在地および準拠法について
  - 5-3 セキュリティインシデントへの対応
    - 5-3-1 責任範囲
    - 5-3-2 通知

---

1 はじめに

本資料は、AOULU CLOUDのご利用を検討されている企業様、または既にご利用いただいている企業様に向けて、AOULU CLOUDのセキュリティ対策への取り組みについてご確認いただくとともに、AOULU CLOUDをより安心・安全にご利用いただくための留意事項をご確認いただくことを目的としています。

また、本資料に記載している内容の対象サービスは以下となります。

- AOULU電子便
- AOULU販売

2 セキュリティ対策

2-1 不正アクセス対策

2-1-1 ネットワーク

2-1-1-1 ファイアウォール

ファイアウォールはシステムを不正なアクセスから守るための装置です。ファイアウォールにて必要最小限のポートのみを許可し、不正な探査やポートスキャンに対する対策を講じています。

2-1-1-2 IPS

IPS（侵入防止システム）を導入し、システムへの不正なアクセスを検知・ブロックしています。

2-1-1-3 WAF

WAF（Web Application Firewall）を導入し、システムへの不正アクセスやWebアプリケーションの脆弱性を悪用した攻撃等を検知・ブロックしています。

2-1-2 サーバ

2-1-2-1 ウイルス対策

ウイルス対策ソフトを導入し、毎日最新のウイルス検出パターンファイルに更新することにより、ウイルス感染を未然に防止しています。

2-1-2-2 不要なサービスの停止

サーバの用途に応じて必要のないサービスを停止し、サーバの要塞化を図っています。

2-1-3 アプリケーション

2-1-3-1 セキュアコーディング

各種脆弱性に対応するため、入力値のサニタイジングやパラメータチェック、SQL作成時のプレースホルダ利用などを開発規約として規定し、遵守しています。

2-1-4 脆弱性対策

2-1-4-1 パッチ適用

セキュリティパッチについて、サービスへの影響や緊急度を確認のうえ、原則月次にて適用を行います。セキュリティパッチの適用状況については一覧表を作成し、適用記録を管理しています。また、緊急の脆弱性が公表された場合のプロセスが明確化され、影響や緊急度を確認し、速やかに対応を行います。

2-1-4-2 脆弱性診断

脆弱性検査については、第三者機関による脆弱性診断を行い、ネットワーク診断（ポートスキャンなどネットワーク層の診断）は日次で実施し、アプリケーション診断（XSS、SQLインジェクションなど）を週次で実施しています。

脆弱性診断の実施および情報の収集を行い、脆弱性が発見された場合には、サービスへの影響や緊急度から優先順

位付けを行い、順次対応を行います。対応に伴い、お客様に影響のある変更を行う場合は、サイト内にて告知を行います。

また、お客様による脆弱性診断は禁止としています。

2-2 暗号化

2-2-1 CRYPTREC 暗号リスト

総務省及び経済産業省にて、電子政府で利用される暗号技術の評価を行い、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」を策定しています。 暗号化を行う際は、このリストに基づいた暗号化方式によって暗号化を実施しています。

2-2-2 通信内容

2-2-2-1 TLS1.2 未満の通信無効化

SSL3.0、TLS1.0、TLS1.1といった脆弱性が存在する古いプロトコルの使用を禁止するため、TLS1.2未満の通信はエラーとして処理しています。

2-2-3 データ

2-2-3-1 機密情報の暗号化

データ保存時の暗号化、ストレージの暗号化、データベース管理システムによる暗号化など、複数の暗号化対策を実施しています。

2-2-4 ハードディスク

2-2-4-1 ストレージシステム

ストレージシステムによりハードディスク全体のデータを暗号化しています。

2-3 物理的セキュリティ

2-3-1 データセンター

安全性の高いパブリッククラウドサービスを利用しており、入退室管理、多要素のアクセス制御、侵入検知など高水準のセキュリティ対策が実施されていることを確認しています。

2-4 ユーザー側管理機能

2-4-1 権限設定

管理者権限を有するユーザーにて、利用者ID（社員）の追加・削除や権限設定が可能です。 利用者毎に利用できる機能やアクセスできる画面を制限可能です。

2-5 セキュリティ強化オプション

企業様のセキュリティポリシーに対応できるよう、セキュリティを強化するためのオプションをご用意しています。 ※ご利用中のサービスによって設定できない場合があります。詳しくはお問い合わせ下さい。

2-5-1 パスワード有効期限

任意の日数で、パスワードの有効期限を設定することが可能です。

2-5-2 セッションタイムアウト

ログイン後、一定時間操作が行われなかった場合に自動ログアウトします。機能のON/OFF、セッションタイムアウトまでの時間の設定が可能となっています。

2-5-3 アカウントロック

一定時間内に連続してパスワードを間違えた場合、一定時間アカウントをロックします。ロック時間やロックまでの回数について変更が可能となっています。

2-5-4 IP アドレス制限

接続元グローバルIPアドレスによる接続制限が可能です。なお、当該サービスはIPv6には対応しておりません。

2-5-5 2要素認証/2段階認証

ID/パスワードでの認証後、ワンタイムパスワードによる認証を追加できます。ワンタイムパスワードはSMSやメールを利用して送信することが可能となっています。これにより、第三者による不正なログインを防止します。

2-6 パスワードポリシー

パスワードは8桁以上15桁以下かつ、英大文字、英小文字、数字、記号から3種類以上を設定することが必須となっています。

2-7 時刻同期

仮想サーバの時間は、クラウドサービスプラットフォームが提供するNTPサービスに同期されています。

3 運用体制

3-1 監視

3-1-1 24時間365日

システムを安定稼働させるため、24時間365日の監視を行っています。

3-1-2 有人監視

有事の際に対応できるよう、有人監視を行っています。

3-1-3 監視内容（死活監視、リソース）、監視間隔

各サーバのリソース監視（CPU、メモリ、ディスク等）やアプリケーション監視を行い、異常を検知した場合はアラートを通知する仕組みを構築しています。

3-2 運用環境

3-2-1 専用 PC

インターネットへアクセスすることができない専用PCからのみVPN経由でサーバへアクセス可能となっています。専用PCはすべての操作ログを取得し作業内容を管理しています。

3-2-2 権限管理

サーバー操作は、弊社情報セキュリティ管理責任者が承認した社員のみが可能であり、専用PCを利用したリモートアクセスにて行います。

3-3 ログの取得について

システムログや操作ログ、アクセスログなど各種ログを取得し、暗号化を行った上で一定期間保存しています。

3-4 特権 ID について

データへのアクセスは弊社の情報セキュリティ管理責任者が承認した社員のみに権限を付与しています。

3-5 CSIRT の設置

年々多様化・複雑化するサイバー攻撃に対して、組織的に取り組む体制を強化するためCSIRTを設置しています。CSIRTでは、セキュリティインシデントの発生に備えた体制整備やセキュリティインシデントの対応、また、外部機関や他社CSIRTとの連携を強化し、自社サービスならびに自社内の更なるセキュリティ強化に向けた活動を行っています。

3-6 監査

3-6-1 システムアカウント

BtoBプラットフォームのシステムアカウントは四半期毎に監査を行い、必要なアカウントのみがシステムへアクセスできるよう制限を行っています。

3-6-2 ログ

システム操作のログを月次で監査し、承認された操作のみが実施されていることを確認しています。また、重要なイベントについてはリアルタイムで通知され、承認されていない操作が行われた際に検知できる仕組みを構築しています。

4 災害対策/障害対策

4-1 データセンター

安全性の高いパブリッククラウドサービスを利用しており、地理的な安全性に加え、冗長電源や消火システムの配備など各種対策が実施されていることを確認しています。

4-2 障害対策

4-2-1 リソース拡張

システムリソースの利用傾向を分析の上、適宜スケールアップやスケールアウトを行っています。

4-2-2 対応フローの整備

システム障害を想定した対応手順書や、対応フロー、体制、連絡網などを整備し、定期的な訓練および見直しを行って

います。

4-3 データバックアップ

4-3-1 取得種別

データベースやアプリケーションを含むシステム全体のバックアップを取得しています。

4-3-2 取得間隔

日次でデータおよびファイルのバックアップを取得、月次にてフルバックアップを取得しています。

4-3-3 保持期間

バックアップの保持期間は6か月です。

4-3-4 遠隔地保存

取得したバックアップは国内遠隔地にて保管しています。

5 コンプライアンス

5-1 認証

5-1-1 クラウドサービス認定

クラウドサービス認定は、一般社団法人クラウドサービス推進機構がクラウドを活用したIT経営の促進を目指し、中小企業の経営者が安全にかつ安心して継続的に利用できるクラウドサービスであることを認定するプログラムです。BtoBプラットフォームはクラウドサービス認定を取得しています。

5-1-2 情報開示認定

情報開示認定制度は、クラウドサービス事業者が安全・信頼性に係る情報を適切に開示している事を第3者が認定し、同一フォーマットで公開することにより、クラウドサービス利用者のサービス比較、評価、選択を支援し安全性向上を目指す制度です。BtoBプラットフォームはASP・SaaSの安全・信頼性に係る情報開示認定を取得しています。

5-2 当社の地理的所在地および準拠法について

当社の地理的所在地はホームページ上の会社概要で定めている通りです。また、システムおよびデータの保管場所は国内に位置し、日本の法律に準拠します。

5-3 セキュリティインシデントへの対応

5-3-1 責任範囲

当社は、主に下記のセキュリティ対策を実施します。

- サイバー攻撃への対策：ファイアウォール、IPS、WAF、ウイルスソフトによる対策を実施
- アプリケーションのセキュリティ対策：セキュアプログラミングを実施
- お客様のデータ保護：暗号化による保護を実施
- バックアップの実施：データ損失やデータ破壊に備えたバックアップの実施
- サービス提供に利用するOS、ミドルウェア：脆弱性情報を確認し、セキュリティパッチの適用やバージョンアッ

プを実施

お客様は、下記のセキュリティ対策を実施するものとします。

- アカウントの管理（必要ユーザーの登録、削除、権限設定、組織管理設定など）
- ID/パスワードの管理（強度の高いパスワードの設定、共有禁止など漏洩対策の実施）
- 利用端末のセキュリティ対策（WEBブラウザのバージョンアップやOSのパッチ適用、ウィルス対策の実施）
- インターネット接続環境のセキュリティ対策（共用Wi-Fiを利用しないなどの対策の実施）

5-3-2 通知

当社がお客様に報告する情報セキュリティインシデントの範囲を以下のように定めます。

- 当社の責任範囲が起因となり、お客様のデータが滅失、棄損もしくは漏洩した場合

お客様への通知はメールやホームページへの掲載など、当社が選択した方法で通知を行います。但し、以下に該当する場合には通知を行わない場合があります。

- 通知することにより、当社やお客様のリスクの増加が考えられる場合
- 当社の情報セキュリティ責任者により通知は行わないと判断される特殊な場合

情報セキュリティインシデントが発生した場合には、可能な限り24時間以内に通知させていただくこととし、状況を確認し当社にて速やかに回復策を実施します。この対応実施による通知内容は逐次更新いたします。また、ご利用のお客様に回復策を実施いただく必要のある場合には、当社より回復策に関する情報を通知します。