やくも水神ネットワーク セキュリティ概要

第2版
作成日： 2025年3月7日
更新日: 2025年8月29日
作成： 小松電機産業 情報システム部

いつも「やくも水神」をご利用いただきありがとうございます。
以下に、やくも水神のサーバー、ネットワーク、監視装置等のセキュリティ対策の状況を記載いたします。今後とも「やくも水神」を何卒よろしくお願いいたします。

当社のやくも水神事業における情報セキュリティマネジメントシステムは、
ISO 27001の認証を取得しています。

ISO27001 認証書のダウンロード

IAS ACCREDITED Management Systems Certification Body
MSCB-113

G-CERTi SYSTEM SERVICE
GIJP-1750-IC
ISO/IEC 27001:2022

1.データセンター（東西２拠点共通）

1. マルウェア対策
    a. やくも水神で稼働している全てのサーバーはアンチウィルスソフトによりマルウェア等から保護しています。
    b. 同様に、ファイル共有機能によりお客様からアップロードされるデータについてもウィルスチェックを行っています。
    c. マルウェアが発見された場合、自動的に管理者へ通知し管理者は原因の究明と対処を行います。

2. データセンター内での通信の監視
    a. データセンター内でのサーバー間、またはサーバーとインターネット間で不審な通信（マルウェア等による通信）が行われていないか常に監視しています。
    b. 不審な通信が発見された場合、自動的に管理者へ通知し管理者は原因の究明と対処を行います。

3. サーバー操作ログの監視・保管
    a. サーバー等の操作ログはリアルタイムに監視しており、当社社員が通常行わない操作が行われていないか常時監視しています。
    b. 不審な操作が行われた場合、自動的に管理者へ通知し管理者は原因の究明と対処を行います。
    c. また、不審かどうかにかかわらず、クラウドシステムに対する全ての操作はログに保管し最低 1 年間は破棄いたしません。

4. アクセスログの監視・保管
    a. ユーザーによる当サービスへのアクセスログを常時取得し 1 年間保管しております。
    b. 不審なアクセスを検知すると、自動的に管理者へ通知し管理者は原因の究明と対処を行います。

5. 定期的なセキュリティアップデート
    a. やくも水神のサーバーは毎月 1 回、セキュリティアップデートを実施し常に最新の状態に保っています。
    b. 定期更新とは別に緊急性の高い脆弱性が公表され、その内容が当社サービスに影響ある場合は直ちにセキュリティアップデートを実施します。

6. バックアップ体制
    a. やくも水神の運用により蓄積した各種データ（施設の状態データ、日報データ、トレンドデータ等）は定期的にバックアップします。
    b. やくも水神ネットワークを構成するサーバー群はサーバーイメージとして定期的にバックアップします。

7. データの暗号化
    a. データベース、ファイル、バックアップデータなど、全てのデータは暗号化して保存しております。

8. データセンター事業者のセキュリティ対策

a. やくも水神を稼働しているデータセンター事業者においては、ISO 27001、ISO 27017、ISO 27018、PCI DSS レベル 1、SOC 1、2、3 など、世界的に認められたセキュリティ保証フレームワークと認定に基づいて適切な技術的で体系的なセキュリティ対策を実装し管理しています。
b. データセンターへの物理的アクセスは、建物の入り口において、サーベイランスシステム、侵入検知システム、その他の電子的システムを用いて、専門の保安要員によって厳重に管理されています。

9. 現場監視装置のセキュリティと閉域網
    a. データセンターと現場監視装置の通信は閉域網で行われインターネットを経由しません。従ってインターネット上の第三者から監視装置に対する直接の攻撃や通信データの盗聴は不可能です。

10. データの冗長化
    a. データベースやファイル、バックアップ、サーバーイメージ等のデータは東西データセンターに冗長化して保存しており、大規模災害やランサムウェア攻撃からサービスを保護しています。

11. データの保管地域は国内に限定
    a. やくも水神のデータは全て日本国内のみに保管しており、海外には保管しておりません。

12. 東西データセンター間の通信
    a. 東西データセンター間の通信にはクラウド事業者が提供する専用線を使用し、インターネット回線は経由いたしません。

2.監視端末（PC等） - データセンター間のネットワーク

1. ここでの監視端末とは、監視画面を提供するPC、スマートフォン、タブレットを指します。

2. 通信の暗号化
    a. PC、スマートフォン等の監視端末とデータセンター間の通信はSSL/TLSにより暗号化を実施しています。

3. 海外からのアクセスの遮断

a. サイバー攻撃の多くが海外のサーバーから行われている事から、やくも水神ネットワークでは海外からのアクセスを全て遮断しています。

4. DDoS攻撃への対応
    a. やくも水神データセンターでは、攻撃がサーバーに到達するより前段でDDoS攻撃への対策を行っております。

5. ファイアウォールによる保護
    a. SQLインジェクションやクロスサイトスクリプティング、既知の脆弱性を狙った攻撃等、外部からの攻撃に対してファイアウォールでサーバーを保護しています。

6. 脆弱性診断（ペネトレーションテスト）
    a. １週間に１回、サーバーシステムに対するペネトレーションテストを実施し、脆弱性レポートの作成と必要に応じて対策を実施しています。

7. メールの保護
    a. やくも水神からユーザーへ送信する警報メールは、SPF（IPアドレスによる送信元確認）、DKIM（電子署名による送信元確認）、DMARC（SPFやDKIMの認証が失敗した場合の対応策の設定）により、なりすましやメールの改竄からお客様を守ります。

8. 通信回線事業者の対応体制
    a. 監視端末 - データセンター間のLTE回線について、関連通信機器を含めてアラート発生時にはただちに当社と情報共有される体制を構築しています。

    b. 当社側から回線事業者へは24時間365日、メールまたは電話での緊急連絡が可能な体制を構築しています。

3.監視端末（PC・スマートフォン・タブレット）

1. パスワード総当たり攻撃への対策
    a. ログインIDとパスワードによる認証に一定回数失敗するとアカウントをロックし、以後は解除するまでの間、正しいパスワードでもログインできません。
    b. ロックの解除はお客様のメールアドレス宛に解除用メールを送信しますので、そのメール内から実施可能です。

2. デバイス認証（スマートフォン・タブレット）
    a. スマートフォン・タブレットでは内部でデバイス認証を行っています。
    b. クラウド側でデバイスの認証枠を設けており、ユーザー様の最初の認証時、デバイスが認証枠に登録されます。
    c. 以降は、認証枠に登録されていないスマートフォン・タブレットからはたとえID・パスワードが正しくてもログインできません。

3. 生体認証
    a. iOSデバイスでは、パスワード認証の他に顔認証・指紋認証による生体認証がご利用いただけます。

4. 2段階認証（PC）
    a. PC監視画面では2段階認証がご利用いただけます。
    b. 2段階認証が有効になっているユーザーでログインする場合、通常のパスワード認証に成功すると登録されているメールアドレス宛に認証コードが送信され、その認証コードを入力するとログインが完了します。

4.インシデント発生時の対応

1. セキュリティ・インシデントが発生した場合は、社内規定に基づき定められた「セキュリティインシデント対応マニュアル」に従って対応いたします。

2. やくも水神のサービスに障害が発生した場合は、社内規定に基づき定められた「やくも水神クラウドサービス復旧計画書」に従って、復旧作業を実施します。

5.災害・火災・停電対策

1. 洪水・水害時にはデータセンターのセンサー等により水の存在を検知し、水を除去する仕組みを備えています。

2. データセンターの立地選定・認定・設計には、海岸の高潮や河川の洪水、大雨、津波等を考慮しています。

3. 火災のリスクを軽減するため、自動火災検知・消火設備を設置しています。

4. 停電が発生した場合、水神が稼働しているデータセンターの電力システムは24時間365日、運用に影響しないよう冗長化と保守が可能な設計になっています。

5. 東京拠点への電力供給は「東京電力ホールディングス株式会社（TEPCO）」が、大阪拠点への電力供給は「関西電力株式会社」がそれぞれ行っています。

6. 東京・大阪の各拠点（各３箇所づつ）は、すべて個別の変電所からの電力供給がされています。

7. すべてのデータセンターに無停電電源装置とバックアップ発電機を備え、停電時にも最低48時間の電力供給が可能です。
    a. それ以上の停電時間の場合、災害の影響によるデータセンターへの燃料搬入経路の状況により異なります。
    b. 長期的な停電をサポートするため、データセンターは燃料供給契約を締結しています。

8. やくも水神が稼働しているデータセンターは、2011年3月の東日本大震災においても障害は発生せず、継続して稼働した実績がございます。

6.責任範囲

1. 当社は以下の範囲において責任を負います。
    a. やくも水神サービスを提供するサーバー
    b. やくも水神の内部ネットワーク
    c. やくも水神のデータセンター内に蓄積されたデータ
    d. やくも水神のセキュリティ体制

2. 以下の範囲については当社責任範囲外となります。
    a. お客様PC、スマートフォンなどのデバイス環境
    b. お客様がご利用の内部ネットワークおよび関連機器（ルータ、無線親機等）
    c. お客様がご利用のインターネット環境
    d. お客様環境のセキュリティ体制
    e. その他、当社が直接関わらない環境

7.その他

1. 社内ネットワークへの侵入の遮断
    a. データセンターに加え、当社ネットワークからデータセンターへの不正侵入を防止するため、以下の対策を講じています。

2. 社員PCの保護
    a. 当社社員が使用するPCには、アンチウイルスソフトおよびセキュリティ強化を目的としたVPNソフトを導入しており、外部からの不正侵入による乗っ取りを防止するとともに、PCからの不審な通信を監視し、必要に応じて通信を遮断しています。
    b. 社内ネットワークにはUTM（統合脅威管理）を設置し、外部からの攻撃や情報漏洩のリスクからネットワークを保護しています。
    c. 社員PCにはデータ記憶領域の暗号化を施し、機密情報や社外秘情報の漏洩防止を図っています。PCの廃棄時には、完全初期化を行うか、廃棄業者による「廃棄証明書」または「データ消去証明書」の取得を義務付けています。
    d. 社員が使用するPCには、定期的なセキュリティアップデートを実施し、常に最新の状態で運用することを義務付けています。

3. 社員へのセキュリティ教育の実施
    a. 当社は社員に対して定期的なセキュリティ研修を実施し、最新のセキュリティ情報（ニュース、脆弱性情報等）の共有を日常的に行っています。
    b. 当社に入社する社員には入社時にセキュリティ研修を義務付け、実施しております。

4. 定期的なセキュリティ審査
    a. ISMSの社内規定に基づき、定期的な内部審査・外部審査を実施します（内部審査は直近で2024年夏に実施済み。公的な審査機関による外部審査は本年4月に第一回を実施予定）

5. サプライチェーンのセキュリティ管理
    a. 当社と取引のあるサプライチェーン全体において、セキュリティ対策状況の確認を定期的に実施しております。

6. ISO27001認定
    a. やくも水神ネットワークを含めた水神事業全体でISMS（情報セキュリティマネジメントシステム）を構築しており、2025年6月にISO27001を取得済みです。