GLASIAOUS＋及び**GLASIAOUS**に関するホワイトペーパー

概要
この文書は当社のクラウドサービス情報セキュリティ方針に基づいて、ビジネスエンジニアリング株式会社が提供する各種クラウドサービスの2023年8月時点における安全管理について記述しています。

クラウドサービスの概要
サービスの内容
ビジネスの成長に寄り添う、クラウド型会計＆ERPサービス

クラウドサービスの所在地と法管轄
ビジネスエンジニアリング株式会社は日本の法人であり、本店所在地は東京都です。当社クラウドサービスの開発、運用は主に日本国内で行っています。またクラウド上のデータはMicrosoft Azure等の第三者クラウドサービスを利用し、海外のサーバ領域にお客さまのデータを保管する場合があります。

クラウドデータの保存	クラウドデータの保存国
Microsoft Azure	日本、東南アジア、東アジア、米国、西ヨーロッパなど

クラウドサービスの開発、運用体制
ビジネスエンジニアリング株式会社は、開発、運用に携わる全ての従業者との間で、機密情報等を私的に利用しないこと、外部に漏洩させないこと等を盛り込んだ機密保持契約を締結しています。また、定期的に社員に対する情報セキュリティ教育を実施しています。

クラウドサービスのバックアップ方法及びバックアップデータの提供
当社は、クラウドサービスの障害に備え、サービス全体に対するデータバックアップを実施しています。バックアップは別のリージョンに移転して保存し、サービス障害時には、迅速にバックアップから復旧できるように備えています。

バックアップ頻度	遠隔地保管
日次	あり

クラウドサービスが基準とする時刻
当社は、クラウドサービス上のデータの完全性のため、次のタイムサーバと同期することで、情報の登録、更新、削除及び各種ログのタイムスタンプの正確性を確保しています。

同期先
Microsoft タイム サーバに同期

クラウドサービスの暗号化
クラウドサービス上のデータについて、万一のデータ漏えいや、内部不正による持ち出し対策として、通信経路やデータに対する暗号化を行っています。

暗号化対象	暗号化
データ	対象
システムとの通信	対象
バックアップデータ	対象

その他のクラウドサービスのセキュリティ機能の提供
クラウドサービス上のデータについて、次のセキュリティ機能をお客様に提供しています。

セキュリティ機能	提供の有無
多要素認証	基本機能として提供
IPアドレス制限機能	基本機能として提供
SSO（シングルサインオン）機能	オプション機能として提供

サイバーセキュリティ攻撃に対する検知
クラウドサービスについては、定期に脆弱性診断を実施しているとともに、次の事項に対するリアルタイム検知の仕組みを導入して、迅速な異常の検出と処置に備えています。

検知対象	対象
ウイルス検知	○
障害検知	○
攻撃検知	○

情報セキュリティインシデントの報告対象及び通知方法
情報セキュリティインシデントの発生により、特定のお客様に影響が出たと判断した場合には、個別に登録いただいているご連絡先に通知いたします。また、サービスの停止等、広くお客様に影響するインシデントが発生した場合には、当社サービスサイト上のトップ画面にて告知いたします。

報告内容	通知方法
サービス障害	メール、サービスサイト

クラウドサービスの障害対応計画の用意
クラウドサービスは、SLAとして年間99.5%以上となるよう、商業上合理的な努力をするものとします。

以上