すべての業務とつながるひろがる
奉行クラウド®

世界トップレベルのセキュリティで、業務をもっと安全に

奉行クラウド
セキュリティ対策ガイド

OBIC BUSINESS CONSULTANTS CO.,LTD.

クラウドに対する一番の不安要素は“セキュリティ”

クラウドの導入を検討する企業の多くが、まず気にするのがセキュリティです。
サイバー攻撃の手口が複雑化する中で、すべてを自社だけで守り続けるのは簡単ではありません。
そのため、自動で最新の防御を更新できるクラウド環境が、安心の選択肢として注目されています。

[オンプレミスとクラウドは、どちらが安全か？]

オンプレミス環境では、**マルウェア感染など端末経由で社内ネットワーク全体に被害が拡大**するリスクがあります。
一方、クラウド（SaaS）はインターネット上の限定されたプロトコル（https等）でのみ接続され、**WAFやFireWallなど多層的なセキュリティ防御**が標準で施されています。
これにより、端末からのマルウェア感染リスクを大幅に低減し、財務データや社員情報などの重要データを安全に保管できます。
クラウド移行は、**セキュリティ強化と運用負荷軽減の両立**を実現する最適な選択肢です。

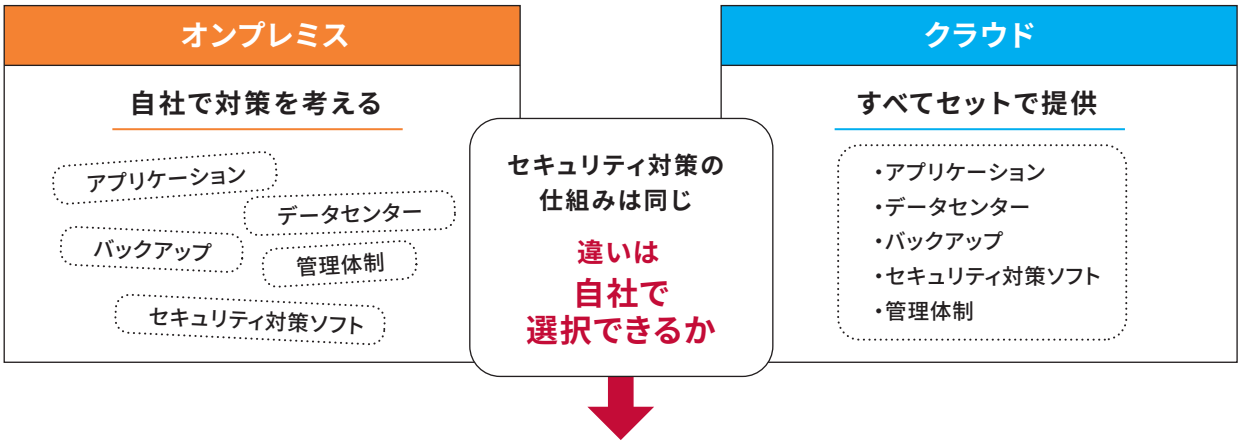
オンプレミスとクラウド（SaaS）のセキュリティ比較

	オンプレミス	クラウド
接続経路	● 社内LANに直接接続 ● 多様な端末がアクセス可能	● インターネット経由で限定的なプロトコル（https等）のみ接続
マルウェア感染リスク	● 端末感染から社内LAN全体へ拡大しやすい	● サービス提供側で、WAF・FireWall等の多層防御 ● 端末からの感染リスクを大幅に低減
セキュリティ対策	● 自社で都度対策が必要 ● 最新攻撃手法への対応が遅れがち	● 常に最新のセキュリティ対策を自動適用 ● 専門チームが24時間監視
データ保護	● 社内サーバーに保存 ● 災害・盗難・内部不正のリスクが大きい	● 厳格なアクセス制御・暗号化・多重バックアップ ● 重要データを安全に保管
運用負荷	● システム管理者の負担が大きい	● 運用・保守はクラウド事業者が実施 ● 自社負担が軽減
	セキュリティは常に自力で対策 固定的で抜け道を探しやすいため攻撃者が侵入しやすい 	**セキュリティは常に最新対応** 常に新しい対策が施されているため攻撃者が侵入しづらい 

攻撃の手段や方法は常に変更するから
最新のセキュリティ対策を継続的に適用できるクラウドがより安全です。

クラウドサービスのセキュリティ対策はメーカー次第
だからこそ、自社で見極めることが大切です

オンプレミス環境では、システムやデータを社内に保有するため、セキュリティ対策やBCP（事業継続計画）対策を自社で実施する必要があります。近年、サイバー攻撃が増加している状況を踏まえると、オンプレミスからクラウドへ移行することは、**セキュリティ強化の有効な手段**となります。
ただし、クラウドサービスであればどこでも良いわけではありません。**セキュリティ対策はメーカー次第**であるため、どのサービスを選ぶかを自社で見極める必要があります。



安全なクラウドサービスを見極めるための
3つのポイント

1 どこで稼働しているか

メーカーのデータセンターやパブリッククラウドなど、様々な選択肢がある中で、どのメーカーのどの場所にソフトウェアを乗せているか。

P3

2 ソフトウェアの対策

提供されているソフトウェア自体のデータが、万が一に備えて暗号化等の対策が実施されているか。

P5

3 運用管理体制

運用管理体制は具体的な対策内容と共に、それをきちんと第三者評価を受けているかを見極めることが重要。

P7

クラウドサービスを選定するうえでの**見極めるポイント**と、
ポイントに沿った**奉行クラウドのセキュリティ対策**をご紹介します。

1 どこで稼働しているか

データセンターの具体的な設置場所（＝国）はどこで、採用しているプラットフォームはどれか

クラウドに保管されるデータの取扱いは、そのデータセンターが設置されている国の法律に依存します。
特に個人情報保護や企業データの管理については、国ごとに適用される法律や規制が異なります。たとえば、海外のデータセンターに保管された場合、その国の法律に基づき、現地政府からデータ開示を求められるケースもあります。日本企業であれば、日本国内でデータが保管されているかを必ず確認しましょう。
そして、データセンターすなわちプラットフォームは、すべてのセキュリティと可用性の土台となります。
物理的な侵入対策や、災害にも対応できる設備、何があっても止まらない仕組みなど、クラウドプラットフォームとして盤石な土台を提供してくれるクラウドベンダー環境でアプリを利用できるのかを確認することが重要です。

データセンター

データセンターの設置場所（＝国）はどこか？

クラウドに保管されたデータは、保管されている国の法律が適用されます。また、災害対策の観点からバックアップが地理的に離れた場所なのかも確認しましょう。

データはどこで保管されている？

プラットフォーム

採用しているプラットフォームはどれか？

障害発生時の対応力やセキュリティ管理、サポート品質などはメーカーによって大きく異なるため、土台となるプラットフォームがどこなのかは極めて重要です。

どのプラットフォームを使用している？

POINT 奉行クラウド

奉行クラウドは、世界トップレベルのセキュリティを誇る「Microsoft Azure」を採用 東日本・西日本にバックアップを計6重化して保管

災害時にもデータを保存する安心のサービス体制に加え、
強固なプラットフォームにより、業務を止めることなく安心して利用できる環境を提供します。

データセンター

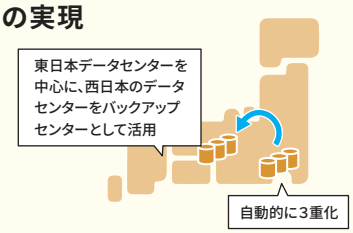
日本国内データセンターのみで運用

日本国内データセンターのみで災害復旧対策を実現

データは国内法が適用される日本国内のデータセンターのみ保管。
東日本データセンターをメインとし、地理的に離れた西日本データセンターをバックアップセンターとして活用することで、お客様のデータを複数の拠点で安全に管理し、予測できない障害や災害発生時にも対処可能なサービス構成を実現。

6重のデータ冗長化による高可用性の実現

お客様のデータは、データセンター内でリアルタイムに3重化されて保管管理されています。ハードウェア障害等が発生した場合は、自動的に正常システムに切り替わりサービスを継続可能です。また、遠隔地データセンターに複製されたデータも3重化されるため、合計6重化して保持します。



プラットフォーム

Microsoft Azure を採用

世界トップレベルのセキュリティ

米国国防総省に次ぐサイバーアタックを防御し、その情報を反映しています。

日本政府が選定したガバメントクラウド

デジタル庁が整備する日本政府共通のクラウド基盤として選定されています。

奉行クラウド　お客様データの管理

仕様項目	仕様
利用データセンター	Microsoftのクラウドプラットフォーム「Microsoft Azure」を採用しています。 日本国内のデータセンターだけを利用し、日本国法に準拠しています。
遠隔地データセンター	東日本データセンターをメインとし、地理的に離れた西日本データセンターをバックアップセンターとして活用することで、お客様データを複数の拠点で安全に管理し、予測できない障害や、災害発生時にも対処可能なサービス構成を実現しています。
お客様データの冗長化	お客様データは、データセンター内でリアルタイムに3重化されて保管管理されています。 ハードウェア障害等が発生した場合は、自動的に正常システムに切り替わりサービスを継続可能です。 また、遠隔地データセンターに複製されたデータも3重化されますので、合計6重化して保持します。
お客様データの暗号化	当サービスに蓄積されたすべてのお客様データは暗号化して保持します。 ※暗号方式には、政府推奨暗号リストに記載されている方式を利用しています。

奉行クラウド　データセンター設備

データセンター事業者

利用データセンター	データセンター事業者／サービス	日本マイクロソフト株式会社 ／ Microsoft Azure
所在地	国名（地域）	日本（関東地域、関西地域）

施設建築物

建物形態	データセンター専用建物か否か	データセンター**専用建物**
耐震・免震構造	耐震構造や免震構造の有無	**有り** 施設の所在地、施設やネットワークの回復能力やサービスのフェイルオーバー手順は、地震活動を含む地域のあらゆる事象の影響を受けにくいように設計されています。 影響回避には、ラックレベルでの分離による免震も含まれます。

非常用電源設備

無停電電源	無停電電源装置（UPS）の有無と、UPSがある場合は電力供給時間	**有り** 施設の所在地、施設やネットワークの回復能力やサービスのフェイルオーバー手順は、地域のあらゆる事象の影響を受けにくいように設計されていて、そこにはUPSシステムや発電機も含まれます。電力供給時間は非公開となります。
給電ルート	別の変電所を経由した給電ルート（系統）で2ルート以上が確保されているか否か（自家発電機、UPSを除く）	**確保されている** 施設の所在地、施設やネットワークの回復能力やサービスのフェイルオーバー手順は、地域のあらゆる事象の影響を受けにくいように設計されていて、そこには異なる系統からの電源供給も含まれます。
非常用電源	非常用電源（自家発電機）の有無と、非常用電源がある場合は連続稼働時間の数値	**有り** 施設の所在地、施設やネットワークの回復能力やサービスのフェイルオーバー手順は、地域のあらゆる事象の影響を受けにくいように設計されていて、電源供給の途絶対応も含まれます。

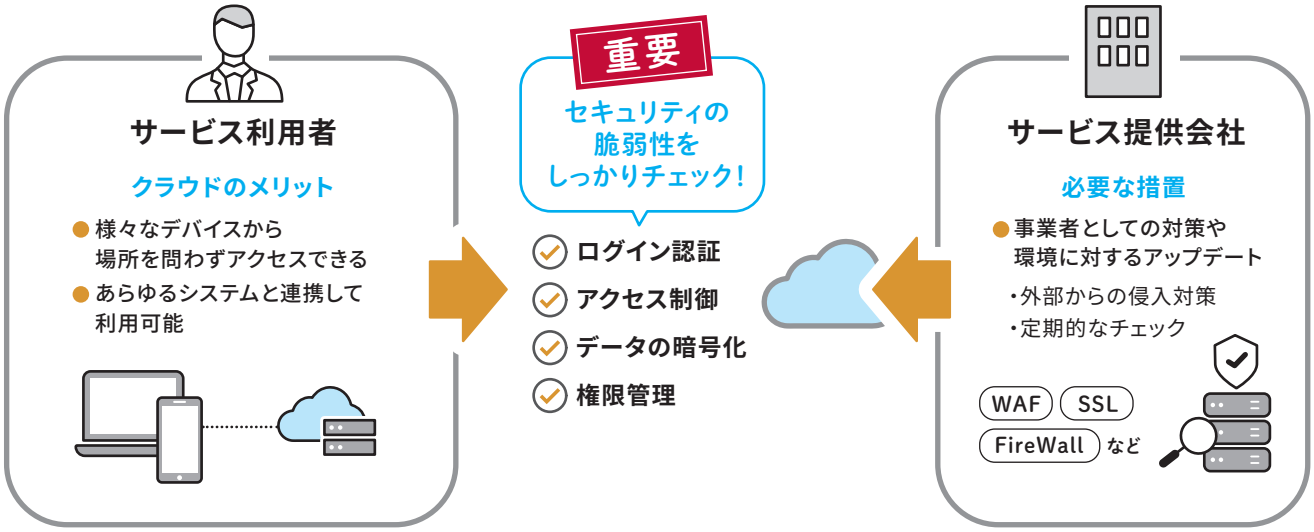
消火設備

サーバルーム内 消火設備	自動消火設備の有無と、 ある場合はガス系消火設備か否か	**有り** 施設の所在地、施設の操業能力、施設やネットワークの回復能力やサービスのフェイルオーバー手順は、運用上考慮すべき事項や地域のあらゆる事象の影響を受けにくいように設計されていて、そこには適切な消化システムも含まれます。
火災感知・報知システム	火災検知システムの有無	**有り**

2 ソフトウェア対策

いつでも、どこでも利用できるクラウドサービスだからこそ、安心して使うためのセキュリティ対策の確認が大切

プラットフォームがいかに強固でも、そのうえで稼働する「ソフトウェア自体」のセキュリティが十分でなければ、全体の安全性は確保できません。ソフトウェアとしては、認証や自社のみが自社データにアクセスできるというアクセスコントロール、データの暗号化、利用者ごとの権限管理などが重要です。
そしてなにより、作成・更新されるソフトウェアにおいては、脆弱性への対処が重要です。定期的な脆弱診断テストがされているか、脆弱性を狙った攻撃へのWAF（Web Application FireWall）による防御などをチェックすることが大切です。



POINT 奉行クラウド

奉行クラウドは、ソフトウェアとしても5つのセキュリティ対策を実施

奉行クラウド独自のセキュリティ対策をプラスして実施することで、お客様の大切なデータをお守りします。

1 アクセス認証

OBCiDによる安心のアクセス

アクセス認証は独自のID管理をOBCiDとして提供します。利用企業ごとに専用の認証ページが用意され、自社利用者のみが自社データにアクセスできます。さらに、複数の奉行クラウドや他のシステムとシングルサインオンを実現することで、利用者の利便性とセキュリティ対策を両立します。

2 データの暗号化

暗号化による強固なデータ保護

データはすべて暗号化され、安全に保管されます。また、奉行クラウドへの通信やデータセンター間の通信など、すべての通信はSSLによって暗号化され、外部からの不正アクセスや盗聴から保護されています。

3 運用監視

24時間365日運用監視

24時間365日、利用状況やリソース状況を自動監視し、障害及び外部からの脅威に対して備えます。

4 WAF＋FireWall

さまざまなサイバー攻撃をブロック

通信経路上には、ファイアウォールによるネットワーク防御に加え、WAF（Web Application Fire）を設置し、WEBアプリケーションへの不正な攻撃も遮断しています。

5 脆弱性診断テスト

定期的なテストで万全の対策を継続

リリース時だけでなく、年1回の定期的な脆弱診断を実施により、脆弱性を徹底的に排除し、万全の対策を継続します。

POINT 奉行クラウド

奉行クラウドは、
利用制御・運用監視などのIT統制基盤をメニューとして提供

アクセスコントロールや権限管理、操作ログなどもお客様自身で細やかに設定・確認が可能なため、
会計などのシステムにおける、IPO検討企業や上場企業の内部統制にも対応しています。

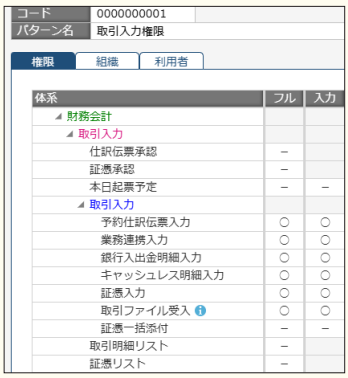
1 セキュリティポリシー

2要素認証　SAML認証

- 厳密なパスワード管理機能（文字数や組合せ等）
- パスワードの有効期限設定
- 指定回数のログイン失敗によるアカウントロック

2 利用者・権限管理

- 承認権限者と担当者の区分け
- アカウント毎に各メニューの使用制限
- 参照許可や削除拒否といった詳細な権限設定



3 ログ管理

- ログイン、ログアウトログ
- メニュー起動、操作に関するログ
- 認証ログ、メニューログ、操作ログの確認

操作日時	法人名	サービス名	メニュー名	操作
2025/10/03 14:25:59	株式会社オービックビジネスコンサルタント	勘定奉行	仕訳伝票入力	終了
2025/10/03 14:25:35	株式会社オービックビジネスコンサルタント	勘定奉行	仕訳伝票入力	メニュー起動
2025/10/03 14:24:44	株式会社オービックビジネスコンサルタント	勘定奉行	仕訳伝票チェック	閉じる
2025/10/03 14:21:09	株式会社オービックビジネスコンサルタント	勘定奉行	仕訳伝票一括修正	メニュー起動
2025/10/03 14:21:06	株式会社オービックビジネスコンサルタント	勘定奉行	仕訳伝票チェック	まとめて修正する
2025/10/03 14:18:01	株式会社オービックビジネスコンサルタント	勘定奉行	仕訳伝票チェック	メニュー起動
2025/10/03 14:17:49	株式会社オービックビジネスコンサルタント	勘定奉行	仕訳伝票入力	閉じる
2025/10/03 14:17:46	株式会社オービックビ	勘定奉行	仕訳伝票入力	登録

奉行クラウド　セキュリティ対策

仕様項目	仕様
ウイルス対策	データセンター事業者にて対応されます。
通信セキュリティ	SSL暗号化通信により、通信データの盗聴、改ざんを防止します。
ファイアウォール	データセンターへの通信経路上に設置します。 また、以下のWebアプリケーション固有のリスクへの対策として、当サービスにおける脆弱性対策とともに、 WAF（Web Application Firewall）を設置します。 ・SQLインジェクション ・クロスサイトスクリプティング(XSS) ・セッションスプーフィング ・XMLベース攻撃 ・ブルートフォース攻撃 ・マルウェアアップロード ・セッション改ざん　など
公的認証等	・プライバシーマーク ・ISMAP ・SOC1（Type2） ・SOC2（Type2）

3 運用管理体制

運用管理体制はメーカーによってさまざまだからこそ、見極めるべきは第三者評価が得られているか

プラットフォームとソフトがいかに優れていても、その運用管理が正しく行われていないと、セキュリティは維持できません。
サイバー攻撃による事件、事故の多くは、運用体制の不備が原因です。運用管理は、システムでは制御しきれず、人が関与するため、これらの内容は目に見えません。目に見えないからこそ第三者の評価を得ているかどうかが確認のポイントとなります。

企業としての運用管理体制

運用管理の例		
	ログ監視・記録管理	システムやアプリケーションの動作記録を監視して異常を検知すること。 不正なアクセスや大量のログイン失敗を検出し、即時対応の体制を整えるなど。
	パッチ管理	ソフトウェアやOSの脆弱性を修正する更新プログラムを適用状態を管理すること。 定期的に実施されているかが重要。
	アカウント・権限管理	利用者ごとに適切なアクセス権を与え、不要なアカウントを削除。 退職者のアカウントなどは速やかに削除し、不要なアカウントを残さないように対策するなど。
	ウイルス・ マルウェア対策の更新	セキュリティソフトの定義ファイルや検知エンジンを常に最新に保つこと。 アンチウイルスソフトの更新などがあげられる。
	インシデント対応手順 の整備	サイバー攻撃が発生したときに誰が何をするかを明確化していること。 社内通報ルールや対策フローを事前に整備するなど。
	教育と啓発	従業員が日常的にセキュリティ意識を高く持つよう教育する。 教育テストなどの定期的な実施が一般的。

自分の目で確認できないからこそ、第三者評価で見極める必要があります！

クラウドサービスの運用体制を評価できる代表的な第三者評価

国際認証SOC1, SOC2

企業が業務を受託したりサービスを提供したりする場合に、その業務に関わる内部統制の有効性について、監査法人や公認会計士が独立した第三者の立場から客観的に検証した結果を記載したものです。

ISMAP

日本政府が利用するクラウドサービスのセキュリティレベルを評価し、政府が求めるセキュリティ要件を満たしているサービスをあらかじめ登録する制度です。この制度は、政府機関がクラウドサービスを調達する際のセキュリティ水準を確保し、効率的な導入を目的としています。

POINT 奉行クラウド

奉行クラウドは、国際認証SOC1,2に加え、日本政府が求めるセキュリティ要件「ISMAP」にも登録

奉行クラウドの運用管理体制について、独立機関（右ページ「奉行クラウドの運用管理体制」参照）による第三者評価を受けており、定期的な見直し・改善を実施しています。

1 SOC1, SOC2 報告書を取得

国際会計基準に準拠した第三者監査評価による財務報告に係る内部統制を対象とした「SOC1 Type2」報告書※1、セキュリティに係る内部統制を対象とした「SOC2 Type2」報告書※2を取得しています。

※1：アウトソーシング事業者が委託されている業務のうち、委託会社の財務報告に係る内部統制の適切性・有効性を対象とした保証報告書

※2：ある一定期間期間におけるクラウドサービス会社のセキュリティの内部統制を評価する保証報告書

2 ISMAPに登録

「政府情報システムのためのセキュリティ評価制度（ISMAP）」において、政府が求めるセキュリティ要求を満たしているクラウドサービスとして、ISMAPクラウドサービスリストに登録されています。ISMAPに登録されているクラウドサービスは、ISMAP運営委員会が定めた厳しいセキュリティ要求基準を満たしています。

3 FISC安全対策基準に準拠

奉行クラウドは、FISC※1が策定するFISC安全基準※2に準拠しています。金融機関をはじめ、FISC安全基準準拠を求めるお客様においても、お客様の重要な業務システム基盤として安心してご利用いただけます。

※1：金融情報センター（FISC：The Center for Financial Industry Information Systems）。
1984年に設立され、金融機関等の情報システムの安全な利活用の推進活動を行う公益財団法人

※2：金融機関等の自主基準としてFISCによって策定され金融機関等の情報システムの安全対策に関するディファクトスタンダードとして活用されている安全対策基準の解説書

奉行クラウド　運用管理体制

● 第三者認定、評価の取得

奉行クラウドの運用管理体制について、下記の独立機関による第三者評価を受けており、
定期的な見直し・改善を実施しています。

- プライバシーマーク
  （一般財団法人日本情報経済社会推進協会（JIPDEC））
- SOC1（Type2）
- SOC2（Type2）
- ISMAP

● 安全管理措置の実施

お客様が奉行クラウドに蓄積する個人情報や業務データを安全に管理するために、安全措置を実施しています。

組織的安全管理措置

管理措置	具体的な対応
運用管理組織の設立	当サービスの運用管理を実施する専門チームを設立し、1名以上の運用責任者を設置します。
運用管理規程の整備	運用管理規程を作成し、運用責任者、運用担当者は本規程に則って当サービスを運営します。 運用管理規程は定期的にその有効性を評価し、必要に応じて見なおし、改善を実施します。
CSIRTの設立	運用管理組織内にCSIRT（コンピュータセキュリティインシデント対応チーム）を設立し、情報セキュリティに関する対応を実施します。

人的安全管理措置

情報取扱者の制限	当サービスの情報取扱者は、部門責任者から承認を得た運用責任者および運用担当者だけに制限しています。
お客様データへのアクセスの制限	運用管理規程により、当サービスの情報取扱者は、お客様データにはアクセスできません。
情報取扱環境	当サービスの運用管理に必要な特権IDやパスワードは、パスワードを設定した電子ファイルで管理し、さらに運用責任者・運用担当者以外は該当電子ファイルにアクセスできないように管理します。
情報取扱者への教育	情報取扱者には、定期的に当サービスの運用管理に必要な弊社所定の教育を実施します。

物理的安全管理措置

作業場所の安全対策	当サービスの運用管理作業は、弊社が定める管理区域内だけで実施します。 ・管理区域は、アクセスが制限された、専用のクラウド上に設置しています。 ・管理区域への接続は、許可されたネットワーク上の、特定の端末だけに制限されています。 ※データセンター事業者における安全管理措置は、P4を参照。
運用端末の制限	当サービスの運用管理作業は、弊社が定める専用端末だけを利用します。 ・管理区域への接続には、VPNソリューションが導入された端末で可能です。 ・管理区域からの、ファイル等情報の持ち出しは、技術的に制限され不可能です。 ※認証等の技術的安全管理措置は、後述の「技術的安全管理措置」を参照。

技術的安全管理措置

認証管理	・お客様環境から当サービスへの利用では、ID／パスワード認証が必要です。 ・弊社による、運用管理では下記の認証を用いています。 ・専用端末利用における、ID／パスワード認証 ・管理区域へのアクセスにおける、VPN利用認証 ・管理区域での作業のための、専用のID/パスワードとSMS認証の多要素認証
SSL/TLS暗号化通信	お客様環境から当サービスへの通信、およびデータセンター内の通信はすべてSSL/TLSで暗号化されて保護されます。
ファイアウォールの設置	お客様環境から当サービスへの通信経路上には、ファイアウォールを設置しています。また、以下のWebアプリケーション固有のリスクへの対策として、当サービスにおける脆弱性対策とともに、WAF（Web Application Firewall）を設置します。 ・SQLインジェクション　・セッションスプーフィング　・ブルートフォース攻撃　・セッション改ざん ・クロスサイトスクリプティング(XSS)　・XMLベース攻撃　・マルウェアアップロード　など
ログの管理	・お客様環境から当サービスへのアクセスについて、すべてのログを管理します。 ・弊社の運用管理では、管理区域内の操作内容すべてを動画にて記録し、ログ管理を強化しています。

仕様項目	仕様
時刻同期	サーバーインスタンスはAzureと時刻同期しており、各サーバーの時間のずれが発生しないようデータセンター事業者にて対応しています。

※ 従業員等の「個人番号」のデータを管理する場合は、暗号化しています。 P10 従業員等の「個人番号」データの取り扱い「技術的安全管理措置」を参照。

奉行クラウドのサービスレベル

以下に定めるサービスレベルを満たすサービスの提供に努めます。
なお、サービスレベルが満たされなかった場合でも、サービス利用料の減免やお客様に生じた損害等の補償は行いません。

可用性

サービス提供時間

仕様項目	仕様	補足事項
サービス提供時間	24時間365日	メンテナンス時間を除きます。
稼働率	99.9%（目標値）	

メンテナンス計画

メンテナンス	実施する場合は、実施の2週間前までに、 電子メール、弊社Webサイト等で告知します。	緊急の場合は、左記に関わらず告知・およびメンテナンスを実施する場合がありますので、あらかじめご了承ください。

バージョンアップ方針

バージョンアップ方針	不定期に実施します。（実施時期は弊社にて決定します） 実施する場合は、実施の2週間前までに、電子メール、弊社Webサイト等で告知します。	緊急の場合は、左記に関わらず告知およびバージョンアップを実施する場合がありますので、あらかじめご了承ください。

サービスの終了

サービス終了時の対応	サービス終了の6ヵ月前までに、郵送および電子メールにて告知します。 お客様のデータは、サービスが終了するまでにお客様の責任で削除、または退避してください。	—

信頼性

システム監視

監視方法	監視システムを利用して、以下の項目に対して監視します。 ・当サービスの死活監視　・パフォーマンス監視　・ログ監視	—

障害対応

障害対応時間	9:00～18:00	国内限定で日本語対応
障害通知	弊社にて障害発生を確認後、速やかに弊社ホームページ、または電子メール等にて通知します。	
問い合わせ対応	弊社サポートセンターにて受付します。 ※お問い合わせ方法や受付時間については、裏表紙「サポート体制」を参照。	—

インシデント対応

対象範囲	以下のインシデントを対象として、予防・検知・対応策を講じます。 ・自然災害　・不正アクセス（不正侵入、DoS/DDoS攻撃など）　・マルウェア感染　・情報漏洩	—
通知	インシデントを検知した際には、利用契約書に定めるオンライン通知等（本サービスの操作画面上又は当社ホームページ上に掲載される当社からのお知らせ又は管理者に対するEメール※の通知）により速やかにお客様に通知をおこないます。	—
予防・検知・対応	○予防・検知　P8「安全管理措置の実施」の4つの管理措置を講じることで、インシデント予防・検知対応を実施します。 ○対応　インシデント事象に応じて、メインデータセンターでのサービス復旧を図ります。自然災害などによりメインデータセンターが利用できない場合は、バックアップデータセンターへの切り替えを行う場合があります。	—
連絡先	インシデント発生に関するご連絡は弊社サポートセンターで承ります。 ※詳細は、裏表紙「サポート体制」を参照。	—

従業員等の「個人番号」データの取り扱い

以下のサービスを利用して従業員等の「個人番号」データをクラウド上に保管することで、漏えい等のリスクを低減できます。

「個人番号」を取り扱うサービス	●『総務人事奉行クラウド』●『給与奉行クラウド』●『法定調書奉行クラウド』●『奉行クラウド HR DX Suite』 ●『奉行Edge 労務管理電子化クラウド』●『奉行Edge マイナンバークラウド』

※当サービスは、JIS Q27001（情報セキュリティマネジメントシステム-要求事項）および、JIS Q 15001（個人情報保護マネジメントシステム-要求事項）に適合した安全管理措置と、「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」に準じた運用管理で、マイナンバー制度に伴う業務への対応とリスクの低減を実現しています。

責任範囲

上記サービスを利用してお客様が特定個人情報を保管・利用するにあたっての、お客様と弊社の責任範囲について記載します。
責任項目については、「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」（平成26年12月11日 個人情報保護委員会発行）の「第4 各論」から引用します。

ガイドラインタイトル	お客様の責任	弊社の責任
第4-1 特定個人情報の利用制限		
(1) 個人番号の利用制限	●	—
(2) 特定個人情報ファイルの作成の制限	●	—
第4-2 特定個人情報の安全管理措置等		
(1) 委託の取扱い	—	—
(2) 安全管理措置	●	▲ ※P8、10「技術的安全管理措置」参照。
第4-3 特定個人情報の提供制限等		
(1) 個人番号の提供の要求	●	—
(2) 個人番号の提供の求めの制限、特定個人情報の提供制限	●	—
(3) 保管制限	●	▲ ※P10「データの管理」参照。
(4) 本人確認	●	—
第4-4 第三者提供の停止に関する取扱い	●	—
第4-5 特定個人情報保護評価	—	—
第4-6 個人情報保護法の主な規定	●	—
第4-7 個人番号利用事務実施者である健康保険組合等における措置等	—	—

〈 責任範囲についての補足 〉

第4-1-(1) [特定個人情報の利用制限]-[個人番号の利用制限]
弊社は、お客様が保管・利用する個人番号にはアクセスできないため、利用できません。

第4-1-(2) [特定個人情報の利用制限]-[特定個人情報ファイルの作成の制限]
弊社は、お客様が保管・利用する個人番号にはアクセスできないため、お客様が保管した個人番号を含む特定個人情報ファイルは作成できません。

第4-2-(1) [特定個人情報の安全管理措置等]-[委託の取扱い]
当サービスは、お客様の個人番号関係事務を弊社が受託するサービスではありませんので、本項は適用されません。

第4-2-(2) [特定個人情報の安全管理措置等]-[安全管理措置]
当サービスにおいて、弊社は個人番号関係事務実施者及び個人番号利用事務実施者に該当しないので本項は適用されません。
しかし、弊社は、お客様が個人番号関係事務実施者として講ずべき特定個人情報の安全管理措置をサポートするために、P8に定める措置を講じます。

第4-3-(1) [特定個人情報の提供制限等]-[個人番号の提供の要求]
当サービスは、お客様の個人番号利用事務、個人番号関係事務を弊社が受託するサービスではありませんので、弊社は、お客様の従業員に個人番号の提供を要求しません。

第4-3-(2) [特定個人情報の提供制限等]-[個人番号の提供の求めの制限、特定個人情報の提供制限]
当サービスは、お客様の個人番号利用事務、個人番号関係事務を弊社が受託するサービスではありませんので、弊社は、お客様の従業員に個人番号の提供を要求しませんし、お客様が保管した個人番号の第三者提供もしません。

第4-3-(3) [特定個人情報の提供制限等]-[保管制限]
弊社は、お客様が個人番号関係事務実施者として講ずべき特定個人情報の安全管理措置をサポートするため、後述「データの管理」に定める方法でデータを管理します。

第4-3-(4) [特定個人情報の提供制限等]-[本人確認]
当サービスは、お客様の個人番号利用事務、個人番号関係事務を弊社が受託するサービスではありませんので、弊社はお客様の従業員等の本人確認は実施しません。

第4-4 [第三者提供の停止に関する取扱い]
当サービスは、お客様の個人番号利用事務、個人番号関係事務を弊社が受託するサービスではなく、弊社がお客様の保管・利用する個人番号の第三者提供を行うものではありませんので、従業員から特定個情報の提供の停止の求めがあった場合であっても、弊社が対応に当たるものではありません。

第4-5 [特定個人情報保護評価]
弊社は、情報提供ネットワークシステムを使用して情報連携を行う事業者ではないため、本項は適用されません。

第4-6 [個人情報保護法の主な規定]
当サービスは、お客様の個人番号利用事務、個人番号関係事務を弊社が受託するサービスではありませんので、弊社が個人情報保護法の個人情報取扱事業者に該当する場合でも、お客様が保管・利用する個人番号を取扱うものではなく、したがって当該個人番号について、弊社が個人情報保護法に基づく義務を負うものではありません。

第4-7 [個人番号利用事務実施者である健康保険組合等における措置等]
弊社は、個人番号利用事務実施者である健康保険組合等ではないため、本項は適用されません。

技術的安全管理措置

管理措置	具体的な対応
個人番号の暗号化	お客様が保管・利用する個人番号は、暗号化および分割して保持します。

※「個人番号」以外の「技術的安全管理措置」は、P8「安全管理措置の実施」を参照。

データの管理

お客様が保管・利用する特定個人情報は、完全独立方式に準拠し、個人情報と個人番号はそれぞれ異なるデータ領域に分けて管理します。
個人番号は暗号化および分割して保持することで、万が一、不正なアクセスがあった場合でも、情報の参照ができないよう管理に努めます。
（分割された断片だけを参照しても、個人番号は参照できません。）

OBCが提供する3つの安心・安全

1 プラットフォーム Azure＋SQL Databaseが提供するセキュリティ

世界トップレベルのセキュリティを誇る「Microsoft Azure」を採用。
強固なプラットフォームにより、業務を止めることなく安心して利用できる環境を提供します。

世界トップレベル セキュリティ

米国国防総省に次ぐ
サイバーアタック防御力で
その情報を反映

日本政府選定 ガバメントクラウド

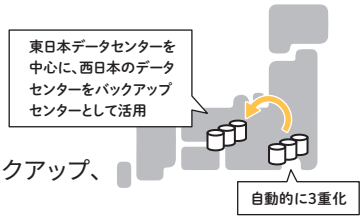
政府が認めた
共通利用クラウド環境

日本国内 データセンター限定 (国内法準拠)

データは国内法が適用される
日本国内データセンターにのみ保管

東日本・西日本 バックアップ (BCP/6重化)

東日本をメインとし、西日本にバックアップ、
それぞれで3重化されます



月間稼働率 99.9%保証 (※Azure SLA)

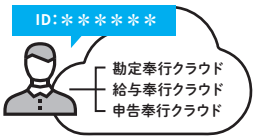
Azureのサービスレベル
アグリメント

2 サービス 奉行クラウドが提供するセキュリティ

奉行クラウド独自の強固なセキュリティ対策により、お客様のデータをお守りします。

OBCiDによる アクセス認証

一つのIDで複数の
奉行クラウドサービスを利用。
シングルサインオン対応



暗号化による 強固なデータ保護

すべてのデータを暗号化。
あらゆる通信をSSLで保護

24時間365日 運用監視

利用状況、リソース状況などを
自動監視。
脅威に対する備えは万全

WAF (Web Application Firewall) +FireWall

WAFにより、
様々なサイバー攻撃をブロック。
FireWallですべてのサービス境界を防御

定期的な 脆弱性診断テスト

リリース時、および年1回の
定期脆弱診断により、
脆弱性を排除

奉行クラウドは、クラウド基盤に、世界トップレベルの堅牢なセキュリティを誇る「Microsoft Azure」を採用。
奉行クラウドならではの強固なセキュリティ対策により、安心・安全な業務環境をご提供します。

3 開発・管理・運用体制 OBCが提供するセキュリティ

運用管理体制について独立機関による第三者評価を受けており、定期的な見直し・改善を実施しています。

SOC1/SOC2
（内部統制/セキュリティ）

国際会計基準による
第三者監査評価

ISMAP
（奉行クラウド、奉行クラウドEdge）

政府情報システムのための
セキュリティ評価制度

ASMツール評価 最高グレード「A評価」を取得
（使用ツール：SecurityScorecard）

外部公表資産の
サイバー攻撃耐性を評価

国内最高レベルの開発・管理・運用体制

ISMAP・SOC＋ASM評価
による運用体制

POINT 奉行クラウド

「データの信頼性」の確保

データの信頼性は最も重要です。Microsoft Azureが提供するクラウドプラットフォーム、SQLデータベース、クラウド開発環境（PaaS）を採用することにより、継続的な「データの信頼性」を確保しています。

研究開発投資の成果を享受

MicrosoftがAIやセキュリティなど新技術に毎年投資する、数千億もの研究開発投資の成果を、奉行クラウド、奉行クラウドEdgeの各製品は自動的に享受することができます。

Windowsアプリの使いやすさ

Windowsアプリを意識したユーザーインターフェースになっており、オンプレミスと同等以上のきめ細かい機能性・操作性を実現しています。

奉行クラウドセキュリティチェックシート

本資料は、『奉行クラウド』『奉行クラウドEdge』『OBCクラウドサービス』（以下、当サービス）における、安全管理措置、サービスレベル、セキュリティ対策など記載した資料です。2025年9月16日時点の情報となります。
予告なくサービス仕様が変更される場合がありますので、あらかじめご了承ください。

本資料は下記のサービスを対象としています。サービス概要やシステム要件などは下記リンク先の弊社ホームページでご確認ください。

サービス	サービス紹介ページ
奉行クラウド	https://www.obc.co.jp/bugyo-cloud
奉行クラウドEdge	https://www.obc.co.jp/bugyo-edge
OBCクラウドサービス	https://www.obc.co.jp/cloud

No.	カテゴリー	対象項目	回答
1	1.基本（クラウド事業者）	会社情報	https://www.obc.co.jp/corporate/outline/profile
2	1.基本（クラウド事業者）	IR情報	https://www.obc.co.jp/corporate/ir/release　財務情報 https://corp.obc.co.jp/ir/financial/situation/
3	1.基本（クラウド事業者）	認証取得状況	・プライバシーマーク：2006年取得、有効期限2026年4月 ・SOC1・SOC2（Type2）：2025年3月取得 ・ISMAP：2025年6月取得、有効期限2026年2月
4	1.基本（クラウド事業者）	セキュリティ評価・監査	・年1回以上の内部監査、外部監査を実施　・年1回以上の脆弱性診断/ペネトレーションテストを実施
5	1.基本（クラウド事業者）	端末・ソフトウェア管理	・社内許可アプリ以外のインストール、使用禁止　・クリアスクリーン、クリアディスクの徹底
6	1.基本（クラウド事業者）	物理セキュリティ	外部データセンターを利用。データセンター事業者側で以下の対策を実施 ・入退館管理体制を整備　・社員証・バッジで社内外を識別 ・個人情報/機密情報エリアへの立ち入り制限　・機器の盗難防止対策を実施
7	1.基本（クラウド事業者）	インシデント対応体制	・書面化された対応計画を策定済み　・インシデント対応部署、調査体制、再発防止策の検討体制を整備 ・CSIRT設置、脆弱性情報の収集/対応を実施 ・全従業員に対し、インシデントや脆弱性の疑いがあれば速やかに管理責任者へ報告する手続きを定めている ・過去1年間、個人データの漏洩等の事案は発生していない
8	1.基本（クラウド事業者）	人権尊重と差別撤廃	・人権リスクの認識と対策　・差別禁止方針と研修、評価制度の見直し
9	1.基本（クラウド事業者）	労働安全衛生管理	労使関係と協定・労働組合等を通じた健全な関係構築　・36協定に基づき従業員代表を毎年選出
10	1.基本（クラウド事業者）	相談・苦情対応体制	・従業員、ステークホルダー向けの相談窓口を設置し、周知
11	1.基本（クラウド事業者）	委託先管理	・選定基準あり。契約時と年1回のヒアリングでセキュリティ/事故歴等を確認　・委託契約には安全管理条項/秘密保持契約を含む
12	1.基本（クラウド事業者）	主な再委託先と役割	・日本マイクロソフト株式会社：データセンター運営（サーバー・ストレージ・ネットワーク基盤） ・株式会社サイバーセキュリティクラウド：WAF運用 ・HENNGE株式会社：メール配信業務 ※再委託先によるお客様データへのアクセスはなし
13	1.基本（クラウド事業者）	機密情報管理	・管理責任者の設置 ・運用担当者は会社に秘密保持誓約書を提出（退職後も有効） ・アクセス権は必要最小限とする　・年1回以上の情報セキュリティ教育を実施
14	1.基本（クラウド事業者）	開発体制	・すべて自社開発。下請け業者なし
15	1.基本（クラウド事業者）	社内ネットワーク管理	・ネットワーク構成図/運用設定方針は手順書で整備済み（非公開） ・社内ネットワークはファイアウォールで防御。未許可機器の接続はEntraIDによる条件付きアクセスで制限 ・ネットワーク機器は管理ツールで管理し、四半期に1回棚卸を実施 ・社外からの直接リモート接続は不可。会社貸与端末からデータセンター内の運用専用端末へ接続
16	1.基本（クラウド事業者）	監査・点検体制	・監査責任者・担当者は独立部門から選任 ・定期/臨時監査を実施し、違反時は改善を実施 ・月次で変更作業ログを確認し、未申請作業の有無をレビュー ・SOC監査にてログ管理体制の評価を受けている ・点検責任者/担当者を選任し、定期/臨時点検を計画的に実施し、規程違反があれば改善
17	1.基本（クラウド事業者）	教育・訓練	・採用時および定期的に教育/訓練を実施　・教育訓練記録を保持し、年1回の見直しを実施 ・年1回、Eラーニングと確認テストによる情報セキュリティ教育を全社的に実施 ・運用管理部門はセキュリティに関する追加教育を実施　・BCP訓練にセキュリティインシデント対応を含む
18	1.基本（クラウド事業者）	通信制御	・TLS1.2以上をサポート　・サーバー証明書によるサーバー認証の実施　・不要なポート・サービスは制限
19	1.基本（クラウド事業者）	責任体制	・サイバーセキュリティリスク管理責任者を設置 ・個人データ管理責任者、各部署の管理者、横断的な調整組織を設置 ・従業者の役割/責任を明確化し、違反時の懲戒処分を就業規則/表彰懲戒規定にて定め
20	1.基本（クラウド事業者）	規程と運用	・個人情報安全管理手順書、情報システム管理規定を整備　・規程に基づく運用、遵守状況の記録/確認を実施
21	1.基本（クラウド事業者）	台帳管理	・取得項目、利用目的、保管場所/方法/期限、管理部署、アクセス制御状況を記載した台帳を整備
22	1.基本（クラウド事業者）	障害・不正アクセス対応	・リカバリ機能、ウイルス対策、不正アクセス対応手順を整備
23	1.基本（クラウド事業者）	盗難・漏えい防止	・機器は施錠/固定、持ち運び時は暗号化/封緘/目隠しシールを使用
24	1.基本（クラウド事業者）	クラウドサービス提供開始時期	・奉行クラウドEdge（例：奉行Edge マイナンバークラウド）：2015年9月～ ・奉行クラウド（例：勘定奉行クラウド）：2016年12月～
25	1.基本（クラウド事業者）	導入実績	・累計導入数：82万以上（2025年8月時点） ・奉行クラウド/奉行クラウドEdge 導入システム数：152,400以上 ・セキュリティインシデントの発生ゼロ（2025年8月時点）・導入事例はこちら https://www.obc.co.jp/casestudies
26	1.基本（クラウド事業者）	データ保管と法令遵守	・サーバはすべて日本国内に設置　・アプリケーションレベルでの顧客データ分離 ・日本国内法に準拠して運用/保管　・管轄裁判所は東京地方裁判所
27	1.基本（クラウド事業者）	サイバー保険	加入済み（2025年8月時点で請求実績なし）
28	1.基本（クラウド事業者）	責任分担	利用契約書に記載。詳細は契約書参照
29	1.基本（クラウド事業者）	稼働率目標	99.9%以上

No.	カテゴリー	対象項目	回答
30	1.基本（クラウド事業者）	データセンター事業者	・データセンター事業者：Microsoft Azure ・サーバ設置場所：日本国内のみ（東日本DC［関東］をメイン、西日本DC［関西］をバックアップ） ・国外アクセス：なし。国外からのアクセス不可 ・データ保存場所：国内のみ。国外移送・保管なし ・データ保存地の法制度：日本法に基づき、制約条件を把握し対応 ・法令対応：日本国内法に準拠。GDPRにおける管理者・処理者はお客様であり、弊社は日本国内での安全管理に努める ・施設の安全設計：雷対策（避雷針・アース）、静電気対策、空調設備の冗長化、異系統電源供給（2ルート以上） ・ティアランク・認証：Tier3相当（JDCC未登録）、FISC・PCI DSS準拠、SOC2など多くの外部認証を取得済み ・自然災害・BCP対策：地理的冗長構成、復旧手順整備、復旧訓練を年1回実施 ・設備変更・廃棄：NIST800-88方式によるデータ消去、上書き処理後に廃棄、履歴は1年以上保管（詳細非公開） ・入退室管理：ICカード等による認証、監視カメラ設置（保存期間は非公開）、物理的入退出装置あり ・サーバールーム管理：施錠・鍵管理、警備員常駐、重要エリアの入退出管理
31	1.基本（クラウド事業者）	システム監視・パフォーマンス・可用性	・死活監視、パフォーマンス監視、ログ監視、エラー監視を5分間隔で実施。異常検知時は運用専任部門に通知 ・障害検知時はWeb掲示/メール通知で告知 ・リソース負荷を定期的にモニタリングし、必要に応じて増強
32	1.基本（クラウド事業者）	ネットワーク・Webセキュリティ	・WAF、IDS/IPS、ファイアウォールを導入 ・不要なサービスは停止、Webフィルタリングで危険サイトへのアクセスを制限
33	1.基本（クラウド事業者）	外部連携・契約管理	・外部組織との契約ではアクセス範囲を明確化し、定期的に監査/レビューを実施 ・情報資産の分類/管理責任者の設定/利用範囲の文書化を実施
34	1.基本（クラウド事業者）	クラウド基盤と復旧体制	・Microsoft Azureを基盤とし、東西データセンターでバックアップを保持 ・年1回以上の復旧訓練を実施
35	1.基本（クラウド事業者）	同時利用可能ユーザー数	契約内容に準ずる。詳細は弊社担当営業までお問い合わせください。
36	1.基本（クラウド事業者）	メール機能・認証・送信ポリシー	・メール送信はTLS対応　・SPF、DKIM、DMARC対応　・メール送信履歴は契約中のみ保持。自由な送信機能はなし
37	2.セキュリティ	認証方式	・ID/パスワード認証に加え、SAML、OpenID Connect、多要素認証に対応 ・グローバルIPアドレス制限により、接続元を制御可能
38	2.セキュリティ	ログの取得と保管	・認証ログ（無期限）、操作ログ（3年）、データ更新ログ（無期限）、メール送信ログ（2か月） ・ログは暗号化され、管理画面から閲覧/エクスポート可能 ・システムログはマルチテナントのため提供不可だが、有事には調査協力可能 ・アクセス/操作/稼働状況の記録/分析を実施　・異常記録の定期確認、監視システムの点検/監査を実施
39	2.セキュリティ	脆弱性診断・ペネトレーションテスト	・データセンター側で年1回のペネトレーションテストを実施 ・アプリケーションは社内の独立部門が年1回以上実施 ・診断結果は非公開だが、重大度に応じて開発部門と連携して対応
40	2.セキュリティ	データアクセスと保護	・利用契約書に基づく目的外アクセスの禁止 ・個人番号等のデータは暗号化して保持 ・開発部門と運用部門の職務分掌実施 ・通信経路の限定、ファイアウォール/WAFによる外部侵入防止 ・従業者の役割に応じたアクセス権限を設定し、必要最小限に限定
41	3.データ管理	暗号化	・通信：SSL/TLS（RSA 2048bit）　・データ：AES256　・個人番号：暗号化＋分割保持（復号不可） ・暗号鍵管理：通信鍵は弊社管理、データ鍵はDC事業者管理。両者ともローテーション・台帳管理あり
42	3.データ管理	バックアップ構成	・遠隔地データセンターに複製実施
43	3.データ管理	業務データの整合性	・登録時に禁止文字のチェックあり。業務整合性はお客様管理
44	3.データ管理	災害時対応	・CSV/Excel形式でのデータエクスポート機能あり
45	3.データ管理	データ返却・削除方法	・お客様自身でエクスポート/削除を実施（利用契約書に準ずる） ・削除証明書：お客様にて削除いただくため、お客様ご自身でご確認ください。 ・記憶媒体の削除：データセンター事業者にて完全削除を実施
46	4.個人情報	お客様業務データの取り扱い 紙、電子媒体の保管ルール	当サービスは業務代行ではないため紙や記憶媒体を利用したお客様業務データの取り扱いはなし
47	5.アプリケーション	推奨環境	裏表紙「推奨環境」を参照
48	5.アプリケーション	パスワードポリシー	・ポリシー設定はお客様にて実施 　・英大文字/小文字/数字/記号のうち3種以上を含む14文字以上の設定が可能 　・ロックアウトポリシー、履歴管理、初回ログイン時の変更強制などに対応 ・パスワードはハッシュ化して保存
49	5.アプリケーション	AI活用・ガイドライン・リスク対応	右記リンク先のAIサービス利用ガイドラインを参照　https://corp.obc.co.jp/ai-guideline
50	5.アプリケーション	セッション管理	・奉行クラウド：セッションタイムアウトなし ・奉行クラウドEdge（ブラウザ利用）：20分
51	6.運用・保守	セキュリティ運用管理	・開発/運用部門の分離、ネットワークはデータセンター内で一元管理 ・運用作業は2名体制/専用端末/操作録画/証跡取得により不正抑止とトレーサビリティを確保
52	6.運用・保守	BCP・災害対策	・地震/火災/大規模障害に備えた業務継続計画（BCP）とリカバリ計画を策定 ・年1回の見直しと実機訓練を実施し、実効性を確認
53	6.運用・保守	メンテナンス	・税制・法改正、機能アップ対応などを不定期に実施　・原則2週間前までに告知（緊急時は即時対応）　・告知はサポートサイトやメールで行う　・プログラム変更は開発部門責任者の承認/テスト/本番環境への反映手順を整備 ・アップデートは拒否不可/併用期間なし（マルチテナント型サービス）
54	6.運用・保守	アカウント管理	・セキュリティカード、ID、パスワードによる本人確認　・アカウント管理手順書に基づき、不正使用防止策を整備 ・運用アカウントは異動/退職時に速やかに無効化　・特権アカウントはポリシーに基づき管理 ・特権IDの発行時審査や定期変更は実施していないが、総務省の指針に準拠
55	7.サポート	サポート体制	・電話/Web問い合わせ　・チャットボット（24時間365日）　・ヘルプセンター（Webヘルプコンテンツ） ・ユーザーコミュニティ（奉行まなボード）
56	7.サポート	サポート時間	・電話・Webお問い合わせシステムに対応　各種問合せ先一覧 | 奉行 Netサービス ・営業時間：平日 9:30～12:00 / 13:00～17:00（日本時間）※年末年始・祝日を除く
57	7.サポート	障害通知のタイミング	・障害検知後、速やかにWeb掲示またはメール通知を実施　・営業時間外の場合は、翌営業日の告知となる可能性あり

「経済産業省」、「ASPIC」、「IPA」が公開するヒアリング形式の資料もご用意しています

こちらよりダウンロードしてご確認ください ▶ https://www.obc.co.jp/hubfs/catalog/BugyoCloud_SecurityCheckSheet.xlsx

推奨環境

PC	奉行クラウド	奉行クラウドEdge		
日本語OS	〈Windows〉 ●Windows 11※1	〈Windows〉 ●Windows 11※1	〈Mac〉 ●OS X 10	「Webアプリケーション」の場合だけ対応 ただし『奉行Edge マイナンバークラウド』の管理者は除く
対応ブラウザ	〈Windows〉 ●Microsoft Edge※2 ●Chrome※2	〈Windows〉 ●Microsoft Edge※2 ●Chrome※2	〈Mac〉 ●Safari※2 ●Chrome※2	「Webアプリケーション」の場合だけ対応
インターネット接続回線	光回線			
解像度	1,366 × 768px 以上			

※1:サポート期間中のバージョン　※2:最新バージョン

スマートフォン/ タブレット	奉行クラウドEdge	
日本語OS	〈iPhone / iPad〉●i OS / iPadOS	〈Android〉●Android
対応ブラウザ	〈iPhone / iPad〉●Safari※3　●Chrome※3	〈Android〉●Chrome※3

※3:最新バージョン

補足事項

● ブラウザ

Cookie、JavaScript、Web Storageを有効にしてください。

● インターネット接続回線

◉SSL 128ビットが利用可能な環境が必要です。ファイアウォールが有効な環境では、アウトバウンド（外向け）に対してTCP 443番ポートで通信できる必要があります。
◉プロキシサーバーをご利用の環境では、当サービスへの接続を許可するようにプロキシサーバーを構成してください。

● スマートフォンでのメール受信

ドメイン指定受信や本文にURL があるメールの受信拒否などの迷惑メール対策をしている場合は、当サービスからのメールを受信できません。弊社ドメイン「@obc.jp」（『奉行Edge 年末調整申告書クラウド』『奉行Edge マイナンバークラウド』の場合は「@obc-service.biz」）を指定受信設定してください。設定方法については、各携帯会社のサイト等でご確認ください。

● 『奉行Edge 給与明細電子化クラウド for 奉行シリーズ』のメール配信

御社のメールサーバーで配信します。メールサーバーの動作環境は、事前に以下のURLにある「メール送信テストツール」を使用して、給与明細を配信予定の全ドメイン名に対して配信テストを済ませておいてください。　https://www.obc.co.jp/payspec/

● 『OFFICE BANKクラウド』

株式会社NTTデータと「VALUXサービス」の契約が必要です。
◉PC名に標準文字（“A”～“Z”、“a”～“z”、“0”～“9”、”-”）以外の記号や全角文字が含まれている場合は運用できません。
◉一括伝送で送信できるファイルの上限サイズは、固定長形式は24MB、XML形式は100MBです。

サポート体制

操作方法等のご質問は、弊社サポートセンターで対応いたします。

お問い合わせ方法	受付時間
お電話でのお問い合わせ	弊社営業日の9:30~12:00　13:00～17:00　※土曜、日曜、祝日、年末年始を除きます。
FAX・オンラインでのお問い合わせ	24時間 365日　※24時間受け付けていますが、17:00以降に送信いただいたお問い合わせは、翌営業日の回答になります。 オンライン問い合わせ先 ： https://www.obcnet.jp/contact/top

お客様無料
ご相談窓口　**0120-121-250**　10:00～12:00 / 13:00～17:00 （土曜・日曜・祝日・当社休業日を除く）

先端技術で未来を創る 株式会社 **オービックビジネスコンサルタント**®
URL https://www.obc.co.jp

〈首都圏〉〒163-6030　東京都新宿区西新宿6-8-1 住友不動産新宿オークタワー30F　TEL.03(3342)1870(代)　FAX.03(3342)1874
〈札　幌〉〒060-0003　札幌市中央区北三条西4-1-1 日本生命札幌ビル10F　TEL.011(221)8850(代)　FAX.011(221)7310
〈仙　台〉〒980-0811　仙台市青葉区一番町1-9-1 仙台トラストタワー20F　TEL.022(215)7550(代)　FAX.022(215)7558
〈関　東〉〒330-0854　さいたま市大宮区桜木町1-11-20 大宮JPビルディング12F　TEL.048(657)3426(代)　FAX.048(645)2424
〈横　浜〉〒220-0011　横浜市西区高島1-1-2 横浜三井ビルディング15F　TEL.045(227)6470(代)　FAX.045(227)6440
〈静　岡〉〒420-0857　静岡市葵区御幸町11-30 エクセルワード静岡ビル5F　TEL.054(254)5966(代)　FAX.054(254)5933
〈金　沢〉〒920-0853　金沢市本町1-5-2 リファーレ5F　TEL.076(265)5411(代)　FAX.076(265)7068
〈名古屋〉〒450-6325　名古屋市中村区名駅1-1-1 JPタワー名古屋25F　TEL.052(589)8930(代)　FAX.052(589)8939
〈大　阪〉〒530-0018　大阪市北区小松原町2-4 大阪富国生命ビル23F　TEL.06(6367)1101(代)　FAX.06(6367)1102
〈広　島〉〒730-0031　広島市中区紙屋町1-2-22 広島トランヴェールビルディング4F　TEL.082(544)2430(代)　FAX.082(541)2431
〈福　岡〉〒812-0039　福岡市博多区冷泉町2-1 博多祇園M-SQUARE 9F　TEL.092(263)6091(代)　FAX.092(263)6099

販売代理店

GP2025.12