ビジネスネットコーポレーション　クラウドサービスレベル基準書

1.9版　　2023/4/1

項目			内容（GooooN）		備考
			通常プラン	トライアル	
事業所概要					
	事業者名	正式名称（商号）	株式会社　ビジネスネットコーポレーション		
	事業所	事業者の本社住所	〒105-0001　東京都港区虎ノ門二丁目10番4号　オークラ プレステージタワー18F		
	認証取得	ISMS認証（ISO/IEC27001:2013）	IS 95618		
		ISMS認証（ISO/IEC 27017:2015）	CLOUD 712752		
サービス基本特性					
	サービス内容				
	サービス提供方針	サービス提供時間	24時間365日（※計画停止を除く）		
		サービスアップグレード方針	計画保守は、年4回程度。		
		サービス提供上のピアクラウド利用	Microsoft Azure AppService（PaaS型クラウド基盤）※プラットフォームのため個人情報の直接取扱いはありません。		
	サービス利用環境	サービスを利用する際の動作推奨環境	【パソコンの場合】 OS：Windows 10 以降 ブラウザ：Edge （最新版） 、 Google Chrome（ 最新版） 【スマホ・タブレットの場合】 OS：iOS（最新版 ）、Android（最新版 ） ブラウザ：Safari （最新版 ）、Google Chrome（最新版）		
	サービスの変更・終了				
	サービス変更・終了時の取扱い	サービス変更、バージョンアップ時の通知期間と告知方法	（1）5営業日前までにWEB又はメールで告知致します。		
		サービス終了時の通知期間と告知方法	サービス終了の半年前までに電話／メール／WEB等で告知いたします		
		サービス終了時のカスタマデータの提供	ご利用者にて管理者画面より各種のカスタマデータをエクスポートする事が可能です。サービス終了前にお客様にて保管下さい。		
個人情報・知的財産権・セキュリティインシデントなどの取扱い					
	個人情報	利用目的の明示、第三者提供、安全管理措置等の取扱い	「個人情報取り扱いについて」を公開しております。		https://www.busnet.co.jp/policy/
	知的財産権	知的財産権に掛かる苦情等の受付	「お問合せ窓口フォーム」又は当社 代表番号により受付けております。		https://www.busnet.co.jp/contact/
	セキュリティインシデント	セキュリティインシデントに掛かる受付	「お問合せ窓口フォーム」又は当社 代表番号により受付けております。		https://www.busnet.co.jp/contact/
		セキュリティインシデント発生時の通知	重大なセキュリティインシデント(情報漏洩等)の発生を当社で認知した段階から可能な限り速やかに通知します。		
		告知方法	メール／WEB／電話等		
契約・機密保持					
	秘密保持	秘密情報条項、契約終了後の秘密保持の取扱い	GooooN利用規約（基本契約）に記載。		https://goooon.busnet.co.jp/pdf/GooooN Usera greement v1 0.pdf
	事故・障害発生時の責任と補償範囲	事故・障害の定義と、その責任範囲、免責条件と内容	GooooN利用規約（基本契約）に記載。		https://goooon.busnet.co.jp/pdf/GooooN Usera greement v1 0.pdf
	サービス解約後のデータ取扱い	サービス解約時のデータ消去	セキュリティに関する補足規約に記載しております。（※契約の終了日から60日以内にサービスご利用上の登録データは完全削除されます。削除されたデータを回復する事は出来ません。）		https://goooon.busnet.co.jp/pdf/sec_amend.pdf
		サービス解約時の事前データバックアップ	ご契約終了前に管理者画面からエクスポートしお客様自らデータを保管下さい。サービス解約後のデータエクスポートは出来ません。		
サポート内容					
	サポート窓口				
	窓口・受付内容	サポート内容	サービスの操作方法等に関するお問い合わせ。	サポートのご提供はありません。販売代理店の営業担当にお問い合わせください。	
		サポート窓口	（1）開通通知の際にご案内しております。 ご契約の主管ご担当者様から、メール／電話で受付。		
		営業曜日、営業時間（受付時間）	平日9:30～17:00（土日祝日、夏季・年末年始休暇期間を除く）		
	サービス通知・報告（変更管理）				
	メンテナンスによるサービス停止通知	定期メンテナンス	平日AM 02:00 ～ AM 02:30の間。※この間はサービスを一時的にご利用出来ない場合があります。		
		告知方法	定期のため事前告知はございません。		
		定期外(臨時)メンテナンス	メンテナンス実施の5営業日前。※緊急の場合はこの限りではありません。		
		告知方法	ログイン画面のお知らせ機能、又はサービスホームページに掲載		
	障害によるサービス停止通知	障害発生	発生から1営業日以内。※営業時間帯においては2時間程度で通知しております。		
		告知方法	サービスホームページに掲載、又はメールにて通知		

項目			内容（GooooN）		備考
情報システムのセキュリティ対策					
	ユーザー認証と管理機能	利用者認証の方法	ログインID・パスワードによる認証		
		ユーザIDの登録方法	（1）管理者ロールIDにより管理者画面からユーザIDの登録が可能です。ユーザIDは社員情報の登録の中で行えます。 登録はcsvによる一括取込方式です。 （2）一般ユーザやユーザIDを持たない場合のID登録は出来ません。管理者の方へID登録を依頼下さい。		
		ユーザIDの削除方法	不要となったユーザIDを削除する事は出来ません。管理者画面から無効化を実施頂くとログイン出来なくなります。IDの完全な削除は、サービス解約に伴うサイト削除により完全に無くなります。		
		IDの権限（ロール）の種類と設定方法	管理者ロールIDにより作成したユーザIDには、機能利用や閲覧範囲を制限できるロールを割り当てる事が出来ます。ロールには管理者ロール、一部の管理機能を限定利用できるロール、一般ユーザのロールがあります。		
		IDロック機能	管理者画面にてIDの有効/無効を設定頂けます。※退職者IDを無効化する事が可能です。		
		初期パスワードポリシー	文字数制限：8文字以上 含有種別：「英大文字・英小文字・数字」3種が含まれている必要があります。 ※ロールによる区別はありません。		
		パスワードポリシーの変更	申込時に初期パスワードポリシーの変更を承る事が可能です。サービス開始後の変更はサポートセンターまでお申込下さい。※初期パスワードポリシーよりも弱いポリシーへ変更する事は推奨しておりません。お申込頂く場合はお客様にてリスクを良くご検討の上でお申込下さい。 ※ポリシー変更はご利用契約URL単位です。変更するとロールに関係無く全てのIDが変更の対象となります。 ※パスワード設定済のIDは、ユーザが新しく変更設定を行った時から新ポリシーが適用されます。		
		初回利用時のパスワード登録方法	（1）管理者ロールID（お申込時にお届け頂いた内容で開通通知書でお客様へ通知されます） →初回ログイン時にパスワード登録が必要になります。ご利用者にて任意の物へ変更頂きます。 （2）管理者ロールIDにより作成した登録ID →各ユーザが初回ログイン時に新規にパスワード設定を行う。（管理者により事前にユーザ初期パスワード設定まで行い配布を行った場合、ログイン時に初期パスワードからの変更が必要になります。ご利用者にて任意の物へ変更頂きます。		
		利用中のパスワード変更の方法	パスワード設定ページからご利用者の方で任意に変更出来ます。 ・初期パスワードポリシーから変更が無い場合は”初期パスワードポリシー”の内容に順じます。 ・初期パスワードポリシーから変更がある場合は、管理者の方へご確認下さい。		
		利用中のパスワード忘れ時の再発行。	ユーザID：、パスワード設定ページからご利用者の方で任意に再設定出来ます。（ご利用者自身で設定する場合はメールアドレス登録が必須です。登録が無い場合はご利用各社様の管理者の方へご依頼が必要です） 開通通知書記載の管理者ID：パスワードを失念し、登録メールアドレスが失効している等でリセットが出来ない場合はサポートセンターまでお問合せ下さい。		
		パスワード誤入力時のロック機能	連続5回パスワード入力を誤ると10分間アカウントがロックされます。		
	お客様データのバックアップ	バックアップ内容と設定	プラットフォームであるMicrosoft Azureのスナップショット機能にて実現しています。 ・完全バックアップ：毎週 ・差分バックアップ：12時間ごと ・トランザクションログバックアップ：5-10分ごと		
		カスタマデータのバックアップ保管期間	最大35日		
		バックアップデータの復元取扱い	取得しているバックアップは、プラットフォームにおける共通障害など運用上における不具合からの回復を目的としております。ご利用者の操作ミスなど、お客様個別の事由による復元には対応しておりません。管理画面の登録データエクスポート機能を利用し定期的に保管下さい。		
	記録（ログ等）の保護	サービスプラットフォーム上で取得される記録（ログ）	（1）サイトへの通信ログ（IP/時間/ブラウザ等のクライアント情報） （2）機能へのアプリケーションレベルアクセスログ（URLやセッション情報）		
		サービスプラットフォーム上で取得される記録（ログ）の保管期間	最大90日　※個別の期間延長や縮小は出来ません。	最大30日　※個別の期間延長や縮小は出来ません。	
		サービスプラットフォーム上で取得されたログのご提供	お客様の監査目的などに限り個別にご提供しております。ご希望の場合はサポートセンターへお申し出下さい。	ご利用頂けません。	
		各ユーザ毎のログイン履歴の取得と閲覧	ID単位でログイン後のトップ画面に前回のログイン日時が表示されます。不正なログインの有無の確認などにご利用頂けます。		
		各ユーザ毎のログイン履歴の保管期間	前回のログイン時間のみ保存されます。		
	セキュリティ対策	ネットワーク分離	サイトはお客様契約(URL)単位で論理的に分離されています。データベースはお客様契約(URL)単位で論理的に分離されています。サイトとデータベースはプラットフォーム内でネットワーク分離されています。		
		IPアドレス制限	ご契約単位(URL)でのみ設定が可能です。ご契約時にお申込下さい。利用開始後はお問合せ下さい。同一ご契約(URL)内で登録されているテナント単位での制限は出来ません。IP制限は1契約(URL)毎に100個まで設定可能です。超える場合は追加の契約をお申込下さい。	ご利用頂けません。	同一ご契約(URL)内テナントをIP制限したい場合は契約を別にして頂く必要が有ります。
		ファイアウォール	装備しています。サービス提供に必要なHTTP/HTTPSのみを公開しています。		
		WAF	装備しています。SQLインジェクション、クロスサイトスクリプティング、OSコマンドインジェクション、パスワードリスト攻撃などのサイバー攻撃を検出する事が可能です。	WAFのご提供対象外です。	
		DoS攻撃・DDoS攻撃対策	プラットフォームに採用しているMicrosoft AzureによるAzure DDos Protection サービスにより対策が実行されています。		https://docs.microsoft.com/ja-jp/azure/security/fundamentals/ddos-best-practices
		コンピュータ・ウイルス対策とパターンファイルの更新間隔	プラットフォームに採用しているMicrosoft Azure によりマルウェア対策がリアルタイムで実行され、常に最新のシグネチャが自動的にインストールされます。		https://docs.microsoft.com/ja-jp/azure/security/fundamentals/antimalware
		セキュリティパッチの適用方針と更新間隔	プラットフォームに採用しているMicrosoft Azure AppService によりOS／ミドルウェアはMicrosoft社のポリシーにより計画的に月例パッチやアップデートがオンデマンドで適用され、常に最新の状態が保たれます。		https://docs.microsoft.com/ja-jp/azure/app-service/overview-patch-os-runtime
		第三者による脆弱性検査など	第三者機関によるアプリケーションに対する脆弱性診断を年１回実施しています。		
	セキュリティを考慮した機能実装	SQLインジェクション対策	社内規定による非機能要件書（自社コーディング規約）に従ったセキュリティ実装により対策を行っています。		
		パスワードハッシュ方式	PBKDF2を採用。（※RSA 研究所の公開鍵暗号化標準仕様の一部で、RFC 2898 として提案されている方法）		
	暗号化対策	通信の暗号化と証明書	SSL（TLS1.2）によりサービスとクライアント（ブラウザ間）は完全に暗号化されます。SSLに用いる証明書は SHA-2(SHA256)に対応しています。		
		データベースの暗号化	プラットフォームに採用しているMicrosoft Azure SQL Databaseによりトランザクションを含めて、クラウドサービスカスタマデータは暗号化されます。		https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-security-overview
		ストレージの暗号化	プラットフォームに採用しているMicrosoft Azure Storageにより、ログやバックアップ等のクラウドサービス派生データは暗号化されます。		https://docs.microsoft.com/ja-jp/azure/storage/common/storage-service-

項目			内容（GooooN）		備考
サービス提供環境					
	プラットフォーム	所在地（リージョン）	Microsoft Azure 東日本リージョン（Japan）によりサービスを提供しています。バックアップデータの一部はMicrosoft Azure 西日本リージョン（Japan）に保管されます。（※リージョンの所在地住所は安全のためMicrosoft社が非公開としております）		https://azure.microsoft.com/ja-jp/global-infrastructure/locations/
	データセンタファシリティ	耐震・免震構造	プラットフォームに採用しているMicrosoft Azureでは、様々な認証基準を満たした堅牢なファシリティ管理が実施されています。 ＊Microsoft Azureは、様々なコンプライアンス認証をクリアしています。 ＊Microsoft Azureは、日本の FISC 安全対策基準の要件を満たしています。 ＊Microsoft Azureは、ISO/IEC 27017:2015を満たしています。		https://docs.microsoft.com/ja-jp/azure/security/fundamentals/physical-security https://www.microsoft.com/ja-jp/trustcenter/compliance/complianceofferings https://www.microsoft.com/ja-jp/trustcenter/compliance/fisc https://www.microsoft.com/ja-jp/trustcenter/compliance/iso-iec-27017 https://azure.microsoft.com/ja-jp/support/legal/sla/app-service/v1_4/
		停電対策（UPS・非常用電源・自家発電装置など）			
		落雷対策			
		火災対策（自動消火設備など）			
		空調管理			
	データセンタ入退館管理	入退室制御システムの有無、入室・退室記録			
		監視カメラ			
		サーバーラックの施錠			
	インフラ可用性対策	ハードウェア冗長性	プラットフォームに採用しているMicrosoft Azure AppServiceによりインフラは冗長性が保たれています。		https://docs.microsoft.com/ja-jp/azure/app-service/overview
		スケーラビリティ	プラットフォームに採用しているMicrosoft Azure AppServiceにより、柔軟なスケーリングを実現しています。		https://azure.microsoft.com/ja-jp/services/app-service/web/
		負荷分散装置の設置等	プラットフォームに採用しているMicrosoft Azureによるロードバランサによる負荷分散とキャパシティコントロールを行っています。	ご利用頂けません。	
	廃棄管理	装置の処分又は再利用	プラットフォームに採用しているMicrosoft Azureにより安全な廃棄が実行されています。		https://www.microsoft.com/ja-jp/download/confirmation.aspx?id=26647
	サービスパフォーマンス管理	アプリケーション、サーバやネットワーク機器等の死活監視	あり		
		システム障害によるサービス応答速度の低下等の監視の有無	あり		
		サービス応答速度等のサービスパフォーマンスの正常性の監視	あり		
サービスの保守運用					
	入退館管理	入退室制御システムの有無、入室・退室記録	当社事業所の作業スペースは、全てIDカードによる入退室管理と記録が行われています。		
	プラットフォームへのアクセス管理	保守要員のアカウント管理	プラットフォームであるMicrosoft Azure へのアクセスは開発運用に必要な人員に特定されています。 プラットフォームへのアクセスアカウントは、社内規定に基づきユニークに権限管理され運用されています。		
		権限設定	プラットフォームの機能リソースへのアクセスは、開発・保守の役割毎に分離され不必要なアクセスから保護されています。 当社保守要員がお客様個別データを閲覧・操作する事は出来ません。		
		操作ログ（アクティビティ）の記録	プラットフォームのリソースへのアクセスや操作記録は、Microsoft Azureの機能により全てアクティビティログが記録されます。記録は全てAzure上で保管されます。		https://docs.microsoft.com/ja-jp/azure/azure-monitor/platform/activity-logs-overview
		操作ログ（アクティビティ）の保管期間	最大90日　※個別の期間延長や縮小は出来ません。		
	保守環境の分離	保守作業環境の分離	メンテナンス上で必要なデータベースへのアクセスは、通常作業環境から切り離された専用端末で実施されています。専用端末へのアクセスは社内規定に基づき安全な方法に制限され、アクセス管理と記録が行われています。		
		保守ネットワークの分離	メンテナンス上で必要なデータベースへのアクセスは、保守専用端末で実施されます。保守専用端末は、通常のオフィスネットワークと分離された専用ネットワークによりプラットフォームへアクセスします。		
	端末セキュリティ	端末セキュリティ対策	保守専用端末へのアクセスは、要員単位で社内規定に基づきユニークに権限管理されています。端末にはウイルス対策ソフト、URLフィルタリングソフトが導入されています。		