当チェックシートは、株式会社Daiの提供するBカートのセキュリティについて「SaaS対応SLAガイドライン」(経済産業省)に基づき回答した資料です。

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
アプリケーション運用					
1	可用性	サービス時間	サービスを提供する時間帯 （設備やネットワーク等の点検／保守のための計画停止時間の記述を含む）	時間帯	提供時間：365日24時間（計画メンテナンス・定期アップデート・セキュリティにおいて必要とされる不定期メンテナンス除く） サポート：平日10:00~17:00
2		計画停止予定通知	定期的な保守停止に関する事前連絡確認 （事前通知のタイミング／方法の記述を含む）	有無	【有】 アップデート前週までにメールで通知・サービスサイト掲載をしております。
3		サービス提供終了時の事前通知	サービス提供を終了する場合の事前連絡確認 （事前通知のタイミング／方法の記述を含む）	有無	【有】 Bカート サービス利用規約 第16条・第17条に添い、ご案内する想定でおります。
4		突然のサービス提供停止に対する対処	プログラムや、システム環境の各種設定データの預託等の措置の有無	有無	【無】 現状、当社開発システム・サービス提供を司る運営システム・現顧客データ管理の第三者委預託の予定はございません。
5		サービス稼働率	サービスを利用できる確率 （（計画サービス時間－停止時間）÷計画サービス時間）	稼働率（%）	現状、SLAの保証提示しておりません。 SLO未定義ながら、現状での回答可能範囲は下記となります。 稼働目標：99.99% 昨年稼働実績（平均）：99.996%、提供環境により異なる
6		ディザスタリカバリ	災害発生時のシステム復旧／サポート体制	有無	【有】 日次バックアップは別環境保存・DBの冗長化を行った上で、データセンター確認結果と復旧見込み次第で別環境への復旧を行います。 該当のロケーションの全てが災害により不通の場合も同じく、別環境への復旧となりますが見込み時間は災害範囲に依ります。 webサーバが故障再起不能となった場合、最短で当日夜間世代のバックアップへのロールバックとなります。 復旧見込み時間は障害原因に依り、短時間で復旧が見込める原因の場合はロールバックは行わず障害直前のデータ状況での復旧となります。 なお、災害による環境復旧費用を契約者へ求める事はございませんが、利用料減額等の措置はございません。
7		重大障害時の代替手段	早期復旧が不可能な場合の代替措置	有無	【無】 完全に現行環境が活きない状態の場合、データアクセスに対する認証・セキュリティを同程度に保った上での提供が望ましく、それ故にバックアップデータから復旧させる事が優先的に考えられます。しかしながらそれは環境復旧を指しますので、この場合代替という提供を想定しておりません。
8		代替措置で提供するデータ形式	代替措置で提供されるデータ形式の定義を記述	有無 ファイル形式	【有】 ●契約者側 CSVデータにて商品・顧客・受注情報を出力する機能があります。また必要があれば、APIにて情報の取得が可能なシステムを提供中です（サービス本体とは別途）。データ出力は契約者にて行っていただきます。 ●当社側 対象データのバックアップ・冗長性をとれる構成をとっておりますが保全性の為であり、契約者が任意に利用可能な機能としてのバックアップ提供はございません。
9		アップグレード方針	バージョンアップ／変更管理／パッチ管理の方針	有無	およそ1～3ヵ月に1回の無償アップデートを提供しております。 緊急度や内容によっては、臨時アップデートを行う場合もございます。 定期アップデート前週までにメールで通知・サービスサイト掲載をしておりますが、機能に関連なくサーバサイドのセキュリティ対策等は契約者への通知なく当社にて行います。
10	信頼性	平均復旧時間(MTTR)	障害発生から修理完了までの平均時間 （修理時間の和÷故障回数）	時間	障害=サーバ・ネットワーク接続障害としての回答となります。 平均10分以下

11		目標復旧時間(RTO)	障害発生後のサービス提供の再開に関して設定された目標時間	時間	12時間以内の復旧を目標
12		障害発生件数	1年間に発生した障害件数／1年間に発生した対応に長時間（1日以上）要した障害件数	回	長時間障害0回（数分単位の通信障害を除く）
13		システム監視基準	システム監視基準（監視内容／監視・通知基準）の設定に基づく監視	有無	【有】 アクセス・負荷・使用量等を別環境のシステムにてチェックし、指定の閾値に到達時に担当者へ通知を行っております。
14		障害通知プロセス	障害発生時の連絡プロセス（通知先／方法／経路）	有無	【有】 監視を踏まえ、特定の閾値を跨いだ際に特定の担当者へメール以外のツールにて開発グループに通知しております。 状況把握の上、大規模な障害発生・システム上重要な動作に関わる事態と判断した際にはメールにて契約者へ連絡させていただきます。 ご連絡は、内容により障害の収束または動作改善を前後することがございます。
15		障害通知時間	異常検出後に指定された連絡先に通知するまでの時間	時間	当社内での通知：数秒～数分 （検知・発信から、開発グループへ着くまでの処理とネットワーク状況にも依存します） 営業時間内/外に関わりません。 営業時間外通知の場合、調査開始時間が通知着信時間と同一でない場合がございます。 契約者への連絡の時間に定めは設けておりませんが、状況把握の上、大規模な障害発生・システム上重要な動作に関わる事態と判断した際にはメールにて契約者へ連絡させていただきます。 ご連絡は、内容により障害の収束または動作改善を前後することがございます。
16		障害監視間隔	障害インシデントを収集／集計する時間間隔	時間（分）	監視対象のデータ性質に依って、頻度の多少がそれぞれにございます。 2~5分 営業時間内/外に関わりません。
17		サービス提供状況の報告方法／間隔	サービス提供状況を報告する方法／時間間隔	時間	機能アップデートは月に一回、通信に関わる重要な情報、B2Bにおける各情報、外部サービスとの連携・プレス、サポート休業日などをサービスサイトまたは管理画面上にて随時確認いただけます。
18		ログの取得	利用者に提供可能なログの種類（アクセスログ、操作ログ、エラーログ等）	有無	【無】 アクセス状況確認等サービス提供上ログを取得しておりますが、あくまで当社の管理・サービス提供の可用性を目的としており、あいにく任意に操作ログをご覧いただく機能は準備がございません。 ただし、管理画面での操作においてのみ任意に確認できる機能を提供しております。
19	性能	応答時間	処理の応答時間	時間（秒）	平均1秒未満。 対象とするページ・ご登録いただくデータ量・接続されている端末のネットワーク環境によって当然に変化の出る点となり、目安としてご把握ください。
20		遅延	処理の応答時間の遅延継続時間	時間（分）	データセンタ内の応答時間が3秒以上となる遅延の継続時間は3時間以内を目標としております。 なお過大なデータ処理の場合・データセンタに依らないプログラム上の処理時間に該当する場合を含みません。
21		バッチ処理時間	バッチ処理（一括処理）の応答時間	時間（分）	任意にご利用いただけるバッチ機能の提供はなく、リアルタイム処理がメインとなります。
22	拡張性	カスタマイズ性	カスタマイズ（変更）が可能な事項／範囲／仕様等の条件とカスタマイズに必要な情報	有無	【有】 任意項目・自由に記載いただくスペースなど多数ご用意しております。機能一覧・マニュアル・オプションをご参照ください。 なお、独自のカスタマイズは承っておりません。
23		外部接続性	既存システムや他のクラウド・コンピューティング・サービス等の外部のシステムとの接続仕様 （API、開発言語等）	有無	【有】 APIを公開しております。仕様につきましては該当サイトをご覧ください。 https://api.bcart.jp

24		同時接続利用者数	オンラインの利用者が同時に接続してサービスを利用可能なユーザ数	有無 制約条件	【有】 リクエスト数とセッション継続数が同一ではないため同時接続をそのどちらかと認識した場合、それらいずれの因果もあるため同時接続可能な最大数は一概では無いながらも、多端末からのアクセスを許可します。 なお他契約者の環境もサーバに存在するサービスとなるため、提供環境のアクセス数に関わらず数の上下の可能性はございます。
25		提供リソースの上限	ディスク容量の上限／ページビューの上限	処理能力	会員・商品の最大数はプランによって上限がございます。 画像データにおいて、極端に多い見込みがある場合（例:商品画像のみで50GBなど）事前にご相談くださいませ。 ページビューにて上限・課金は設けておりません。
サポート					
26	サポート	サービス提供時間帯（障害対応）	障害対応時の問合せ受付業務を実施する時間帯	時間帯	メール受付：365日24時間受付 電話窓口：平日10:00~17:00 ※年末年始・夏季休暇・社員研修期間を除く ※重大な障害発生の場合、営業時間外に連絡をさせていただくことがございます
27		サービス提供時間帯（一般問合せ）	一般問合せ時の問合せ受付業務を実施する時間帯	時間帯	メール受付：365日24時間受付/営業時間外受付時:回答翌営業日 電話窓口：平日10:00~17:00 ※年末年始・夏季休暇・社員研修期間を除く
データ管理					
28	データ管理	バックアップの方法	バックアップ内容（回数、復旧方法など）、データ保管場所／形式、 利用者のデータへのアクセス権など、利用者に所有権のあるデータの取扱方法	有無内容	【有】 データの管理・バックアップは契約者にて行っていただきます。 契約者側：CSVデータにて商品・顧客・受注情報を出力する機能があります。また必要があれば、APIにて情報の取得が可能なシステムを提供中です（サービス本体とは別途）。データ出力は契約者にて行っていただきます。 当社側：対象データのバックアップ・冗長性をとれる構成をとっておりますが保全性の為であり、契約者が任意に利用可能な機能としてのバックアップ提供はございません。なおバックアップは保管が単一のロケーションとならぬよう稼働環境とは別環境へ取得し、また当バックアップデータからの復旧が可能であることを確認しています。
29		バックアップデータを取得するタイミング(RPO)	バックアップデータをとり、データを保証する時点	時間	当社責任による万が一の障害発生時には当日夜間（時間帯と内容によっては前日夜間）へのロールバックが最短となります。 しかしながら、契約者操作によりデータ破損した際は契約者取得のバックアップにて管理していただくことになります。
30		バックアップデータの保存期間	データをバックアップした媒体を保管する期限	時間	障害用バックアップデータにつきましては、2週間以前のデータは当社では保持しておりません。 契約者によるバックアップ・帳票出力は契約者管轄にて管理いただきます。
31		データ消去の要件	サービス解約後の、データ消去の実施有無／タイミング、保管媒体の破棄の実施有無／タイミング、およびデータ移行など、 利用者に所有権のあるデータの消去方法	有無	【有】 契約期間満了日の翌日に削除させていただきます。記憶媒体はデータセンタで管理しており、契約者の解約毎の媒体破棄は行っておりません。 満了日に管理画面にログインしていただき、出力可能な機能の範囲にてCSVデータの出力をお願い致します。
32		バックアップ世代数	保証する世代数	世代数	14世代
33		データ保護のための暗号化要件	データを保護するにあたり、暗号化要件の有無	有無	【有】 データは暗号化された領域に格納しております。
34		マルチテナントストレージにおけるキー管理要件	マルチテナントストレージのキー管理要件の有無、内容	有無 内容	【無】 当社システムにて管理しており、契約者側へのキー提供・契約者が認識する事象はございません。具体的な処理・構成につきましてはセキュリティ上非公開とさせていただいております。 なお、マルチテナント下において利用される領域はデータベース含め分離されています。

35		データ漏えい・破壊時の補償／保険	データ漏洩・破壊時の補償／保険の有無	有無	【有】 加入済みです。 利用規約に定める範囲において補償を行います。
36		解約時のデータポータビリティ	解約時、元データが完全な形で迅速に返却される、もしくは責任を持ってデータを消去する体制を整えており、外部への漏えいの懸念のない状態が構築できていること	有無 内容	【有】 データ出力は機能範囲で契約者側にて行っていただきます。 報告は、削除を行った旨をメールでご案内しております。削除後の非存在の証明は難しいですが、ご希望いただきましたら出力結果が存在しないという出力はご案内可能です。
37		預託データの整合性検証作業	データの整合性を検証する手法が実装され、検証報告の確認作業が行われていること	有無	【有】 実装前にテスト段階を開発グループ外で行い、処理の整合性確認に努めております。 また幾パターンかのフィルタを通す事で検知・遮断、またその状況を確認できる仕組みを構築しております。
38		入力データ形式の制限機能	入力データ形式の制限機能の有無	有無	【有】 入力制限にてエラーメッセージ及び不審な入力に対しアクセス遮断する動作を有します。
セキュリティ					
39	セキュリティ	公的認証取得の要件	JIPDECやJQA等で認定している情報処理管理に関する公的認証（ISMS、プライバシーマーク等）が取得されていること	有無	【有】 ISMS認証取得済：IS 705947 ISO (JIS Q) 27001 準拠
40		アプリケーションに関する第三者評価	不正な侵入、操作、データ取得等への対策について、第三者の客観的な評価を得ていること	有無 実施状況	【有】 外部によるアプリケーション、プラットフォームに対するペネトレーションテストを実施しております。
41		情報取扱い環境	提供者側でのデータ取扱環境が適切に確保されていること	有無	【有】 アクセス可能な従業員は限定され、その権限・認証を認知する者を限るとともに構成・経路は非公開とさせていただきますが条件成立のためのロケーション・認証を設けております。
42		通信の暗号化レベル	システムとやりとりされる通信の暗号化強度	有無	【有】 ご利用いただく環境は~sslv3,~tlsv1.1無効にしております。接続可能なブラウザにご注意をお願いいたします。 なお暗号化スイートにつきましては随時安全性が疑わしくなったものを除外しております。
43		会計監査報告書における情報セキュリティ関連事項の確認	会計監査報告書における情報セキュリティ関連事項の監査時に、担当者へ以下の資料を提供する旨「最新のSAS70Type2監査報告書」「最新の18号監査報告書」	有無	【無】 情報セキュリティに対する事項・体制は、監査を含めISO27001に適うレベルのプロセスをとっております。契約者任意の会計監査ならびに監査基準に対する資料提供・監査受け入れは原則的に行っておりません。また、監査報告書の公開はしておりません。
44		マルチテナント下でのセキュリティ対策	異なる利用企業間の情報隔離、障害等の影響の局所化	有無	【有】 分離した権限を発行し領域ごと提供しており、データベース含め分離した構成をとっております。が、コントロールにおいては非公開情報とさせていただいております。
45		情報取扱者の制限	利用者のデータにアクセスできる利用者が限定されていること、利用者組織にて規定しているアクセス制限と同様な制約が実現できていること	有無 設定状況	【有】 アクセス可能な従業員は限定され、その権限・認証を認知する者を限るとともに構成・経路は非公開とさせていただきますがロケーション・認証を設けております。
46		セキュリティインシデント発生時のトレーサビリティ	IDの付与単位、IDをログ検索に利用できるか、ログの保存期間は適切な期間が確保されており、利用者の必要に応じて、受容可能に期間内に提供されるか	設定状況	【有】 1従業員1IDで管理システムの認証を行います。 契約者へログの提供はあいにく行っておりませんが、万が一セキュリティインシデント発生の際には当然に影響範囲特定に必要な情報提供・調査にあたる認識でおります。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	定義ファイル更新時等。
48		二次記憶媒体の安全性対策	バックアップメディア等では、常に暗号化した状態で保管していること、廃棄の際にはデータの完全な抹消を実施し、また検証していること、USBポートを無効化しデータの吸い出しの制限等の対策を講じていること	有無	【有】 接続権限を成立させるには特定の条件を必要とします。条件は非公開事項とさせていただきます。 前提として、バックアップを外部記憶媒体保存する必然性を産まない運用をすることにより、外部記憶媒体に保存を許可しておりません。

49		データの外部保存方針	データ保存地の各種法制度の下におけるデータ取扱い及び利用に関する制約条件を把握しているか	把握状況	データセンター、当社ともに日本国法に準拠します。
当社補足事項					
50	データセンター	データの所在地	サーバーおよびデータ保管先の所在地はどこか。	所在地	【有】 国内リージョンのデータセンター利用にて提供しており、国外リージョンへの個人情報の格納は予定にございません。所在地はデータセンターのセキュリティ上非公開となっております。 データの格納先には、ISO27001ならびにISO27017の認証取得済みであるアマゾンウェブサービスジャパン株式会社(AWS)の提供するデータセンターを利用しております。
51		データの再委託	各顧客データ・顧客が入力したデータ取扱いの第三者委託はあるか。	有無	【無】 当社開発システム・サービス提供を司る運営システム・現顧客データ管理の第三者委預託はございません。
52		データセンター入館管理	入退室管理されたコンピュータルームの施錠管理されたラック等、明示的に許可された者以外は触れない環境に設置されているか。	有無	【有】 ※ AWS リスクとコンプライアンス より https://aws.amazon.com/jp/compliance/resources/ 物理的セキュリティ統制には、フェンス、壁、保安スタッフ、監視カメラ、侵入検知システム、その他の電子的手段などの境界統制が含まれますが、それに限定されるものではありません。AWS SOC レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。 ※SOC3report https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf
53		データセンター監査	ユーザーによるデータセンター訪問、監査を受け付けるか。	可否	【否】 ※ AWS リスクとコンプライアンス より https://aws.amazon.com/jp/compliance/resources/ いいえ。AWS のデータセンターは複数のお客様をホストしており、幅広いお客様が第三者による物理的なアクセスの対象となるため、お客様によるデータセンター訪問は許可していません。このようなお客様のニーズを満たすために、SOC 1 Type II レポートの一環として、独立し、資格を持つ監査人が統制の有無と運用を検証しています。 ※SOC3report https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf
54	セキュリティ	脆弱性への対応	セキュリティパッチを適用する等、サーバの脆弱性対策を遅滞なくかつ定期的に実施しているか。	頻度	サーバサイドと提供サービスにおいて随時必要なパッチまたはシステムアップデートを行なっております。突発的に発生するCriticalな攻撃難度/事例や深刻度、公式patchが無い場合の手動対応等はそれらの影響度から判断し行う為、定期性を持たせない実施としております。 また、変更内容に依ってはテスト等の検証を経るため一概に即時適用を行いませんが、懸念される特定のCVE番号をお伝えいただければ対応済みか非対応かの回答は可能です。
55		アクセス経路の制限	ファイアウォール等のアクセス制御を行い、公開する必要のない通信ポートは閉じているか。	有無	【有】 詳細は非公開とさせていただきますが、レイヤー毎に必要範囲の通信を許可するよう制御しております。ネットワーク/トランスポート層においてもFW等以外に経路に依る遮断など複数の制限を行なっております。
56		不正なアクセスに対する対策	侵入・改ざん・Dos攻撃を検知し制御する仕組みがあるか。	有無	【有】 外部会社提供のIDS,IPS,WAFの他、FW含め複数の遮断のシステムを稼働させ攻撃を検知、該当トラフィックの制御等を実施しております。
57		不要な表示の有無	公開する必要のないディレクトリ・ファイル・設定情報は外部から不可視とし、必要のない機能は、停止する等の措置がされているか。	有無	【有】 公開ディレクトリまたはレスポンスにおいて、各ミドルウェアの設定またはwebアプリケーションにおいて停止もしくは非表示等にしております。 またプロセスの起動制限済みです。

58		セキュリティ検査	公開前にセキュリティ検査を実施し、提供に適した状態であることを確認し報告を提出できるか。	有無	【有】 リリース前のコードレビュー、該当技術者以外によるアドホック含む社内テスト、不定期に外部セキュリティ会社によるアプリケーションに対するペネトレーションテストを実施しております。いずれのテストにおいても、テスト内容/脆弱性結果/修正内容の公表、提供はしておりません。
59		ログの保持	利用者の活動、セキュリティ事象と関連するログ期間はどのくらいか。	期間	期間はログの種類にもより6ヶ月～、重要な証左となるものは2年間保持しております。
60	体制	内部不正についての対策1	人的な対策はどのようなものを行っているか。	対応状況	入社時および年数回のセキュリティ情報を教育・周知しております。内容は時事情報・取扱注意点・影響範囲・懲戒なども含み、試験を通しセキュリティリテラシー向上に努めております。 採用においては関連法令、規制及び倫理に従って行い、候補者が情報セキュリティに関する役割を果たすために必要な力量を備えているかの観点をふまえ選考しております。
61		内部不正についての対策2	従業員が契約者のデータへ不必要に、許可なくアクセスすることへの抑止力はあるか。	対応状況	該当情報へは特定経路や特定システム経由でのアクセスとなる仕組みを準備し、またそれを認識できる従業員と管理者を限定しております。 その範囲内において、データベースの可用性維持・アップデート・サポート上等の必要性からデータベースへのアクセスが発生する事はご了承いただく点となりますが、その際のアクセスの抑止はルール上のみではなくシステムを介したと制限となります。 なお、規程にて懲戒を設けております。
62		個人情報取り扱い	個人情報の取扱い業務があるか。	有無	当社はデータの保存・保守、システム提供を行うサービスであり、 契約者及びエンドユーザが入力した個人情報の取り扱い業務（取り扱い代行業務含む）は行っておりません。 サービス提供時のサポート上またはアップデート等によりデータへのアクセスを伴う事象はございますが、 サービス提供目的の範囲内であり、またそのアクセスには複数の制御をもって実施しております。
63		内部事故についての対策	データの持ち出し・紛失への対策はあるか。	対応状況	お預かりしているデータ自体を、外部記録媒体への保存・持ち出しを不許可、紙媒体での持ち出すことは理由に適わないため紙媒体への出力は許可されません。 他業務においては社用の外部記録媒体のみ許可し、許可のない私物のストレージは禁止です。 紛失というインシデントに予防線は張れないため、デバイスのアクセス自体に認証・セキュリティ管理者にて対処可能なよう保存領域を分離し、連絡を要点におき周知しております。
64		ユーティリティ表示	現在のシステム稼働状況を視認できるページは準備されているか	有無	【無】 障害発生時、リアルタイムに稼働状況を確認できるページの提供をしておりません。障害時の通知はメールにて行わせていただいております。 またサービス提供環境はサポート受付環境と分離しておりますので、お電話・メールにてお問い合わせいただくことが可能です。
65		セキュリティ領域の確保	オフィスの物理的セキュリティ領域を設け、出入りを管理しているか。	有無	【有】 オフィスにおいて情報を取り扱う業務においてはセキュリティエリアを設け、該当領域へ立ち入りする人物は識別し入退室管理されています。
66		セキュリティに関する外部からの指導	契約者の指示による情報管理体制の改善等の指導を受け入れられるか。	可否	【否】 セキュリティ向上のための改善を継続的に行う中で、実施に伴った効果が当社も共に見込まれ、管理運用やコストを許容できる際には当然に改善されるべき認識でおります。 しかしながら前提としてISMS(ISO27001)の要求事項を全て満たしているものとご理解いただき、ISO規格外の契約者独自のセキュリティポリシー適用、当社の管理ポリシー・ルールの公開、実現と結果報告要求の受け入れは原則出来かねることを、ご了承ください。

67		事故発生時の外部監査	セキュリティインシデント発生時、契約者による外部監査を受け入れられるか。	可否	【否】 該当領域への契約者による立ち入り監査は他契約者の情報取扱の観点からできかねます。 当社責による重大な漏洩事案があった場合には外部のセキュリティチェックを実施することとなり、契約者へのシステム自体・システム構成など技術的情報の公開は致しかねます。ただし万が一当社責による漏洩を伴う重大なセキュリティインシデント発生の際には当然に影響範囲特定に必要な情報提供と調査にあたる認識でおります。
68	機能	パスワード定期変更	パスワードに有効期限を設け、再発行を強制する仕組みがあるか。	有無	【無】 パスワード定期変更機能の提供予定は、現状ございません。
69		パスワード強度	十分な強度のパスワード文字列が設定できるか。	有無	【有】 会員が設定するパスワードを、桁,文字類の組み合わせ等でのパスワードポリシーの設定が可能です。管理画面においては、契約者のパスワードポリシーに適うパスワードを利用環境のマスター管理者の責任の元で設定をお願いいたします。
70		多要素認証	ID/PW以外の本人認証の仕組みを設けているか。	有無	【無】 多要素認証機能の提供予定は、現状ございません。
71		アカウントロック	一定回数ログインに失敗した場合に、アカウントを無効化またはロックする機能が提供されているか。	有無	【有】 一定時間内の一定回数の失敗で一定時間のアカウントロックしておりますが、回数/期間は非公開とさせていただいております。
72		アクセス制限	利用環境において、第三者がアクセス出来ない仕組みがあるか。	有無	【有】 管理画面においては、IP(v4)制限をかける機能を提供しております。
73		アクセス権限管理	管理者毎のアクセス権限を制御する機能があるか。	有無	【有】 管理画面ログイン後の閲覧・編集など作業可能な権限を任意に付与する機能がございます。

回答補足	該当事項において、それぞれ資料をご参照ください。			
事項	文書名	資料		
機能詳細	Bカートユーザーガイド	https://userguide.bcart.jp/		
アプリケーション層	IPAセキュリティ実装チェックリスト	https://bcart.jp/faq/detail/276/		
禁止事項/免責	Bカート利用規約	https://bcart.jp/company/terms/		

Ver4.0