助ネコ EC 管理システム

セキュリティホワイトペーパー

第 1.1 版

2023 年 6 月 21 日

株式会社アクアリーフ

目次

読みたい項目をクリックすると該当先のページにジャンプします。

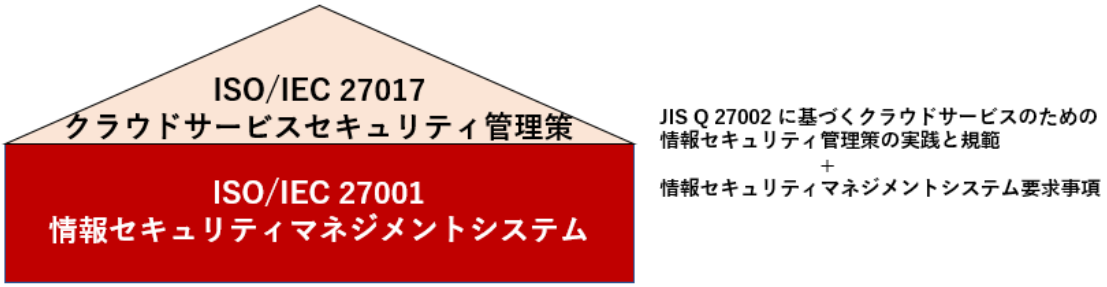
1 はじめに

1.1 セキュリティホワイトペーパーの目的

「助ネコ EC 管理システム セキュリティホワイトペーパー」(以下、本書)は、クラウドセキュリティの国際規格(ISO/IEC 27017 : 2015)で求める要求事項に対して、クラウドサービスプロバイダ(CSP)が実施する管理策をご確認いただくことを目的としています。

ISO/IEC 27017 は、情報セキュリティ全般に関するマネジメントシステム規格である ISO/IEC27001 の取り組みを ISO/IEC 27017 で強化した管理策のガイドライン規格になります。本書では、このガイドラインの”情報セキュリティ管理策の実践の規範”箇条 5～18（17 箇条を除く）に沿って管理策を記載しています。

【27001、27017 の関係図】



1.2 本書の適用範囲

本書の適用範囲は、助ネコ EC 管理システム（日本国内向けサービス）となります。尚、助ネコ EC 管理システムで提供する機能の詳細に関しては、以下サイトを参照下さい。

・助ネコ EC 管理システムサイト … https://www.sukeneko.com/

２助ネコ EC 管理システムについて

2.1 助ネコ EC 管理システムとは

株式会社アクアリーフがネットショップ向けに通販管理業務ソフトウェアを提供する SaaS(Software as a Service)型のクラウドサービスです。

本サービスには、「受注管理」「発注管理」「在庫管理」「商品登録」などを行う業務システムがあります。

お客様のニーズに合わせて、それぞれの業務システムを単独で、組み合わせて、全てをまとめて導入することが可能です。

また、以下の機能も合わせてご利用できます。

・ 助ネコアプリ …… スマートフォンでバーコード読取や売上状況の確認
・ Web 領収書 …… 購入者が Web 上から領収書の PDF でダウンロード

【各サービスの特徴・強み】

① 【受注管理】

「業務の効率化」と「リピーター育成」の実現

ネットショップの受注処理を自動化し、業務の効率化とリピーター育成を同時に実現できます。一括メール送信、配送先住所や商品情報により運送会社を自動選択、住所の誤りを識別、リピーターを判別し購入回数に応じた処理、フォローメール送信等の接客機能が搭載されています。

② 【在庫管理】

「売り越し」と「販売機会の損失」の防止

複数のネットショップの在庫数を連動し、「売り越し」や「販売機会の損失」を防ぎます。セット商品の在庫数管理、発注点をメールで報せるアラート機能など、在庫数管理の効率化をサポートする各種機能が搭載されています。

③ 【商品登録】

「一括編集・一括出品」と「アップロード予約」

複数のネットショップへの出品作業を、助ネコ上に作成した商品マスタにて一括で行えます。アップロード時間の予約も可能です。セール時や商品棚卸時の複数商品情報の一括編集も簡単に行えます。商品マスタは出品済のデータを取り込み、簡単に作成できます。

④ 【発注管理】

「発注数の予測」と「自動発注」

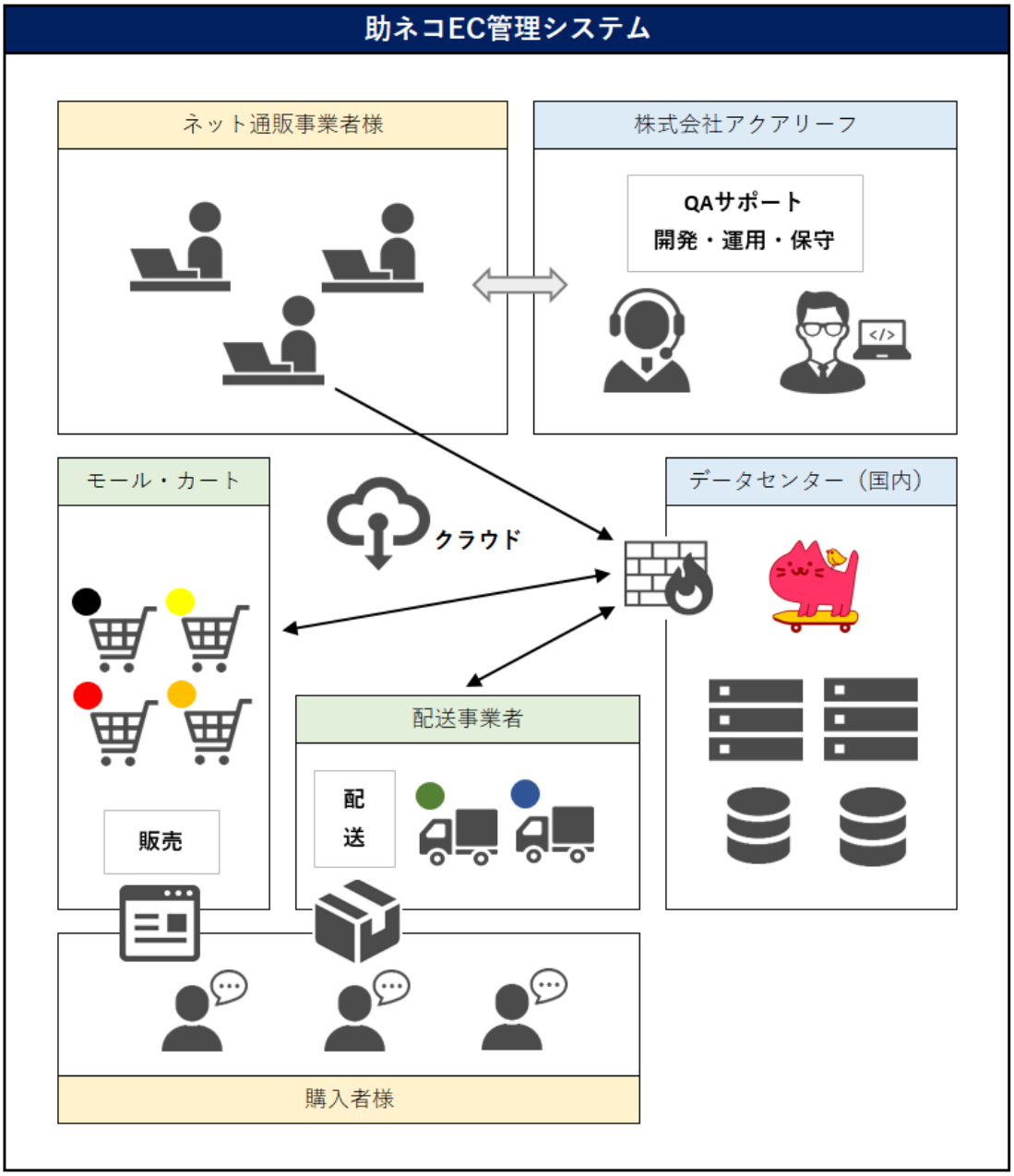
助ネコの商品マスタから発注書を簡単に作成できます。【在庫管理】との併用により、在庫数が少なくなったタイミングでの自動発注や、過去の販売実績から発注数を予測するなど、経験に頼りがちだった発注業務をサポートする機能が揃っています。

【受注管理】との連携で、注文後に発注をかける受発注処理ができます。

⑤ 分かりやすいインターフェースとサポート

システムが苦手な方でも、直感的に利用できるインターフェースが特徴です。管理画面には、処理タイミング毎に必要な操作ボタンのみが配置されています。また、コンサルティング力の高いサポートも高く評価されており、初めてのシステム導入でも安心してご相談いただけます。

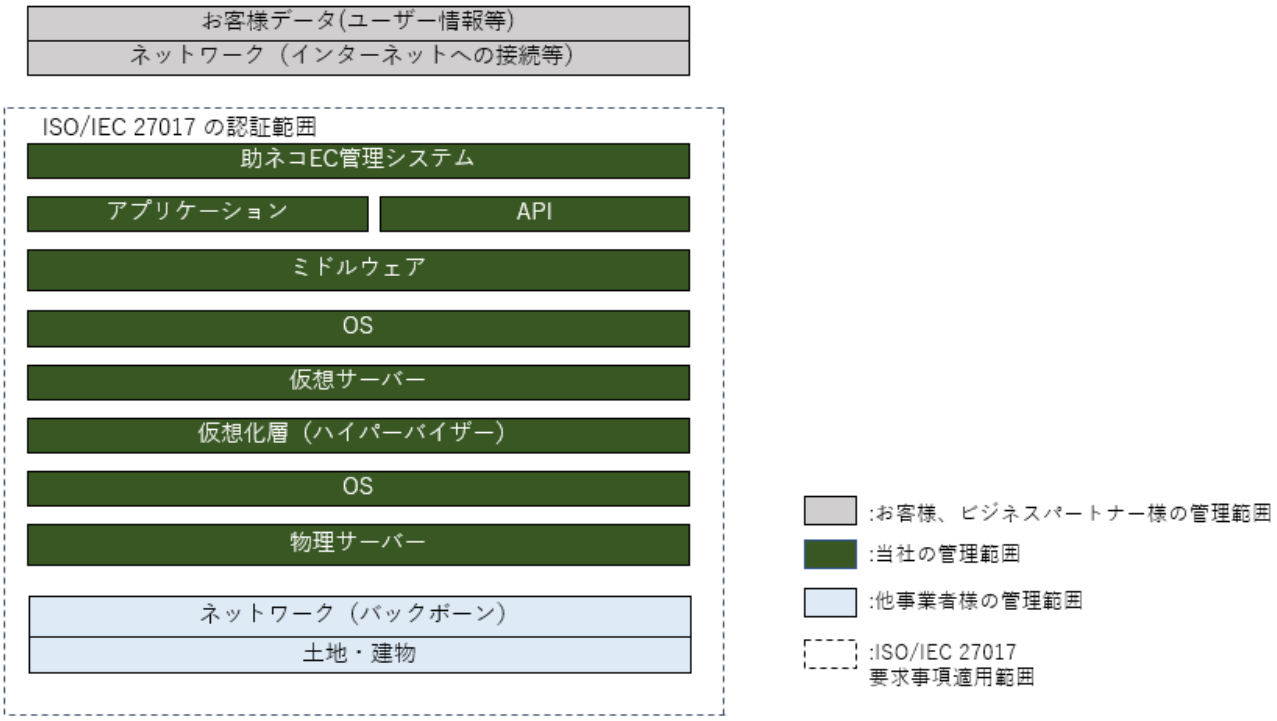
【サービス提供イメージ図】



2.2 責任分界点について

助ネコ EC 管理システムに関する責任分界点は、以下になります。

【責任分界点の図】



3 JIS Q 27017 : 2016 (ISO/IEC 27017 : 2015) への対応

3.1 助ネコ EC 管理システムの管理策(3.2 節)に関する見方の説明

3.2 節で、JIS Q 27017:2016(ISO/IEC 27017:2015)が求める要求事項に対する管理策を記載します。「5.1.1 情報セキュリティのための方針群」 などの番号・タイトルは、ISO27017 が求める”情報セキュリティ管理策の実践の規範”箇条 5～18（17 箇条を除く）の小項目番号・要求事項原文を示し、後に続く内容は、助ネコ EC 管理システムの要求事項に対する解釈及び管理策になります。

3.2 助ネコ EC 管理システムの管理策

5.1.1 情報セキュリティのための方針群

クラウドサービスプロバイダ(CSP)は、クラウドサービスの提供及び利用に取り組むため、情報セキュリティ基本方針を拡充することが求められています。助ネコ EC 管理システムでは、弊社の情報セキュリティ基本方針に従いサービスを運用しています。

・情報セキュリティ基本方針 … https://www.aqualeaf.co.jp/security-policy/

6.1.1 情報セキュリティの役割及び責任

助ネコ利用規約 及び 本契約時の「助ネコ EC 管理システム 重要事項の説明（必読)」にて契約やサービスの内容を定義し、サービス提供を実施しています。

また、サービスご利用中に発生する QA 等の問い合わせ対応に関しては、申込時に合意いただいた「助ネコ EC 管理システム 利用規約」にてサービスの内容を定義し、サービス提供を実施しています。

・サービス利用規約 … https://www.sukeneko.com/terms/

尚、土日、深夜などのサポート時間外に「管理画面に接続できない」「データの取り込みができなくなった」「在庫連動ができていない」等の不具合が発生した際には、本契約時にご案内する「サーバートラブル・システムトラブル専用連絡先メールアドレス」までご連絡下さい。システム管理者が確認のうえ、調査・対応を致します。

※連携先側に起因する障害等は、弊社で即時解決ができない場合があります。

6.1.3 関係当局との連絡

弊社の所在地は、神奈川県平塚市八重咲町 7-28　神奈中八重咲町ビル 4F となります。
・弊社 Web サイト・企業情報 … https://www.aqualeaf.co.jp/company/

尚、助ネコ EC 管理システムで保存いただくデータの所在は、日本国内にある、情報セキュリティ格付ランク「AAAis(トリプル A)」を取得し、最新テクノロジーを結集し、クラウド時代に対応した国内の最高水準のデータセンターで管理しています。不正なアクセス制限・免震・耐火設備を備え、停電時には自家発電装置が稼動し、24 時間 365 日有人監視が行われています。

※情報セキュリティ格付とは、マネジメントの成熟度、脅威に対する対策の強度、
コンプライアンスへの取り組みなどの視点から総合的に評価されるものです。
その中で「AAAis(トリプル A)」とは、17 段階中、最高ランクの格付けです。

CLD.6.3.1 クラウドコンピューティング環境における役割及び責任の共有及び分担

助ネコ利用規約 及び 本契約時の「助ネコ EC 管理システム 重要事項の説明（必読)」にてサービスの内容を定義し、サービス提供を実施しています。また、サービスに関するお問い合わせ先に関しては、助ネコサポートにて受付を行っています。
尚、責任分界点に関しては前出の「2.2 責任分界点について」を参照下さい。

7.2.2 情報セキュリティの意識向上、教育及び訓練

情報セキュリティ要件の周知徹底とクラウドサービスの運営ルール徹底を目的として、全ての従業員を対象とした教育・訓練及び意識向上の策を実施しています。ISMS 研修、倫理・行動規範研修、サーバー・インフラ研修、部門別セキュリティ研修、BCP 研修及び訓練、外部講師による企業人研修を受け、理解度テストやアンケート、レポート提出を通じ、セキュリティセンス向上に努めています。また、日々の作業ログが記録されていることを全員が認識して業務を行っています。

8.1.1 資産目録

お客様の情報資産(保存データ)とサービス提供者である弊社が運営するための情報資産は明確に分離しております。
尚、助ネコ EC 管理システム上にお客様が作成・保存する情報資産は、お客様の管理範囲となります。

CLD.8.1.5 クラウドサービスカスタマの資産の除去

本サービスの提供が終了した場合に、お客様が作成・保存した情報資産（保存データ）に関しては、利用規約に記載された内容に従って 90 日以内に破棄するものとします。弊社にて取得した情報資産（保存データ）のバックアップについても合わせて破棄致します。但し、お客様の情報資産を含まないサービス共通ログは対象外とします。

お客様側で情報資産のバックアップ等が必要となる場合には、助ネコマニュアルに記載された内容に従って対応を実施して下さい。

8.2.2 情報のラベル付け

ご利用いただく助ネコ EC 管理システムの機能の詳細に関しては、各種マニュアル類も含めて 助ネコシステム内に公開しています。

システム内にご登録いただいた情報に関しては、(モール別/注文ステータス/カテゴリ/注文処理タイプ)による情報のラベル付けをしております。

9.2.1 利用者登録及び登録削除

助ネコ EC 管理システム開始時にご契約いただいた内容に従って、管理者権限を有する利用者 ID をご提供致します。提供した利用者 ID にて業務運営に必要となる利用者の登録・更新・削除の機能がご利用いただけます。

提供機能の利用にあたっては、操作マニュアルを参照下さい。

9.2.2 利用者アクセスの提供（provisioning）

利用者の権限管理機能を提供しています。

9.2.3 特権的アクセス権の管理

助ネコ EC 管理システムの利用にあたっては、利用者 ID、パスワード認証による多段階認証技術を利用しています。

9.2.4 利用者の秘密認証情報の管理

助ネコ EC 管理システムの初期利用時には、管理者権限を有する利用者 ID・パスワード及び起動のための手順をメールにてご連絡させていただいております。

パスワード変更にあたっては、マニュアルを参照下さい。

9.4.1 情報へのアクセス制限

助ネコ EC 管理システムのご利用にあたっては、各種業務の管理権限を有している利用者によって機能制限を行うことができます。

9.4.4 特権的なユーティリティプログラムの使用

全てのサービス利用においては、認証が必要となっており、セキュリティ手順を回避し、各種サービス機能の利用を可能とするユーティリティプログラムの提供は行っておりません。

CLD.9.5.1 仮想コンピューティング環境における分離

1）シングルテナント環境の場合

仮想化環境を利用し、アプリケーション・オペレーティングシステム・ストレージ及びネットワークの論理的分離を実施しています。

2）マルチテナント環境の場合

マルチテナント環境では、ユーザーID によるアクセスの分離を実施し、別テナントへの不正アクセスを抑止しています。

CLD.9.5.2 仮想マシンの要塞化

構築するすべての仮想化環境は、ポート・プロトコル・IP アドレスへの制限を実施しています。

10.1.1 暗号による管理策の利用方針

TLS1.2 による情報の暗号化によるデータ盗聴や改ざんの防止と、ファイアウォールの導入による外部攻撃からのネットワーク防御はもちろんのこと、WAF（ウェブアプリケーションファイアウォール）の導入により、Web サービスにおいて最も攻撃をされる可能性の高い、Web サーバに対する各種攻撃の防御も行っております。

各種業務のお客様パスワードはハッシュ化しています。すべての「個人情報」は、AES 方式（Advanced Encryption Standard）での暗号化を行い、データベースに保存されます。

11.2.7 装置のセキュリティを保った処分又は再利用

機器の老朽化、故障等により交換した機器媒体の処理については、アクアリーフの内部規定に基づき適切に廃棄処理を行っています。ハードディスクの物理破壊、または、廃棄証明書の取得を行います。

12.1.2 変更管理

提供するサービスの変更を実施する場合、影響のあるお客様に変更内容を、助ネコサポート、助ネコシステム内のお知らせ、メールでのご案内を通じて行います。

12.1.3 容量・能力の管理

安定的にサービスを提供するため、各テナントのキャパシティを明確にし、日々の運用プロセスの中で稼働監視を行っています。監視の結果として必要と判断された場合には、適切なタイミングにて、システムメンテナンスを実施します。

CLD.12.1.5 実務管理者の運用セキュリティ

ご利用いただく助ネコ EC 管理システムの操作方法に関しては、各種マニュアル類も含めて助ネコシステム内に公開しています。

12.3.1 情報のバックアップ

お客様が実施可能なバックアップ機能として、受注データをダウンロードする機能があります。弊社の行うシステム及びお客様の大切な情報資産のバックアップに関しては、弊社サーバ内で厳重に管理、常時バックアップ（レプリケーション方式（数秒～数十秒ごとの）バックアップ）を行っております。さらに、毎日深夜に 1 回、購入者様情報の全バックアップを行っています。

また災害に備え、購入者様情報に関するデータは、メインのデータセンターとは別の場所（国内）に第二のデータセンターを用意しディザスタリカバリを行っています。障害復旧時点は前日バックアップ取得時点となります。

12.4.1 イベントログ取得

弊社の責任範囲において、クラウドサービスの維持管理に必要となる適切なログを取得しています。保管期間は原則 6 か月です。6 か月を経過したログは順次削除させていただきます。

※個人情報保護の観点から、 6 か月以内に削除する場合や、法令順守の為、6 か月以上ログを保存する場合もございます。

お客様において、ログが必要な場合は、弊社問い合わせ窓口（助ネコサポート）までご連絡下さい。

12.4.4 クロックの同期

助ネコ EC 管理システムで利用する、物理・仮想サーバは日本国内 NTP サーバを参照することで時刻を同期します。システム内で表示されている日付と時刻（処理履歴等）

は、日本標準時間です。毎日 23：59 に、データセンターの NTP サーバと日本時間の時刻同期を行っています。（お客様が使われるパソコン等の時刻設定は、お客様ご自身でお願い致します。）

CLD.12.4.5 クラウドサービスの監視

ネットワークのトラフィック及び、CPU・メモリ・ディスクアクセスの使用率増加を検知する監視は、弊社が実施しております。現在、結果をお客様に公開できるサービス機能は有しておりません。監視結果が必要となる場合においては、弊社問い合わせ窓口（助ネコサポート）までご連絡下さい。

12.6.1 技術的ぜい弱性の管理

IPA のメールを確認後、社内の技術者で検討し、適用するか否かを判断しています。お客様で対応が必要となるぜい弱性情報があった場合には、助ネコサポートよりご連絡致します。

助ネコ EC 管理システム側での対応が必要になった場合には、緊急メンテナンスにて対応を実施し、メンテナンス前後で対応内容及び対策後結果を随時連絡致します。

13.1.3 ネットワークの分離

ネットワークの仮想化技術を利用し、他のお客様とのネットワークの分離を適切に行っています。

また、サービス提供者である弊社の社内ネットワークと助ネコ EC 管理システム側のネットワークとは、物理的に分離されています。

CLD.13.1.4 仮想及び物理ネットワークのためのセキュリティ管理の整合

物理ネットワークと論理ネットワークの整合性がとれるように設計、構築、管理を徹底しています。

14.1.1 情報セキュリティ要求事項の分析及び仕様化

情報セキュリティに関しては、情報セキュリティ基本方針及び、助ネコ HP、本書に記載しています。

下記に主なセキュリティ機能を記載します。詳細は本書の該当項番をご参照下さい。

・アクセス制限機能（9.4.1 情報へのアクセス制限、CLD.9.5.2 仮想マシンの要塞化）
・通信暗号化機能（10.1.1 暗号による管理策の利用方針）
・バックアップ機能（12.3.1 情報のバックアップ）
・ログ取得機能（12.4.1 イベントログ取得）

14.2.1 セキュリティに配慮した開発のための方針

助ネコ EC 管理システムは、社内のコーディング規約に基づいて、また IPA が発行する「安全なウェブサイトの作り方」を参考に開発しています。また、外部の専門会社による、日々の動的アプリケーションスキャン、年 1 回の Web 脆弱性診断にてセキュリティ対策を実施しています。

他に、Amazon 米国本社指定の監査法人によるリスク監査を受け、「カリフォルニア州消費者プライバシー法 2018 年（CCPA)」に基づく Amazon の「適正利用規約」「データ保護ポリシー」の要求事項に対応しています。

15.1.2 供給者との合意におけるセキュリティの取扱い

助ネコ EC 管理システムは、SaaS(Software as a Service)型のクラウドサービスとなり、責任分界点の詳細に関しては前出の「2.2 責任分界点について」を参照下さい。

また、助ネコ EC 管理システムのセキュリティ対策に関しても「2.2 責任分岐点について」に記載する弊社サービスの提供範囲において必要なセキュリティ対策を実施しています。

15.1.3 ICT サプライチェーン

他のクラウドサービスの供給は受けておりません。助ネコ EC 管理システムの提供に必要となる構成要素(データセンターや機器等)の供給については、弊社セキュリティ方針を満たすようリスク管理を実施しています。

16.1.1 責任及び手順

弊社で確認できたセキュリティインシデントに関しては、情報セキュリティ基本方針に則り、適切に対応しております。

また、確認できたセキュリティインシデントが、情報漏えい等お客様に重大な影響を及ぼす可能性がある場合においては、検知から 72 時間以内に助ネコサポートより通知致します。

16.1.2 情報セキュリティ事象の報告

システムやサーバのトラブル時のお客様への告知は、助ネコシステムにログインできる場合には、お知らせ画面での通知、ログインできない場合は、Twitter による通知を行っています。

お客様からの緊急対応、トラブル対応へのお問い合せには、専用の連絡メールアドレスを提供しています。ご利用にあたっては本契約時の重要事項記載書類もしくはシステム内のお問い合わせページを参照下さい。

16.1.7 証拠の収集

裁判所からの開示請求など、法律に基づいた正当な開示請求が行われた場合、お客様の同意なく、お客様のデータを第三者に開示することがあります。

18.1.1 適用法令及び契約上の要求事項の特定

助ネコ EC 管理システムの利用に関して、適用される「準拠法」は「日本法」となります。

18.1.2 知的財産権

助ネコ EC 管理システム上でサービスをご利用いただく上で知的財産権に関わるお問い合わせは、助ネコサポートへお問い合わせ下さい。

18.1.3 記録の保護

弊社の責任範囲において、お客様アクセスログを取得しています。必要な場合は、弊社問い合わせ窓口（助ネコサポート）までご連絡下さい。

尚、保存期間は 6 か月間となります。

18.1.5 暗号化機能に対する規制

お客様が利用するサイトでは TLS による通信の暗号化を使用しています。尚、輸出規制の対象となる暗号化の利用はありません。

18.2.1 情報セキュリティの独立したレビュー

社内内部監査、マネジメントレビュー、年度リスクアセスメントの実施に加え、外部セキュリティ会社よる定期的な Web 脆弱性監査（プラットフォーム診断 及び アプリケーションの脆弱性チェック）や、ISO/IEC 27001、ISO/IEC27017 の ISMS 認証取得の取得において第三者による審査を受け、情報セキュリティに対する取り組みを行うことで、常に安全なセキュリティレベルを確保しています。

更新履歴

版数 日付 更新内容
第 1.0 版 2023/05/22 初版公開
第 1.1 版 2023/06/21 改訂