統合顧客管理(CRM)システム Synergy!

セキュリティに関するホワイトペーパー

2024 年 1 月 31 日

シナジーマーケティング株式会社

更新履歴

日付	更新内容
2023/10/31	作成
2023/12/12	・誤植修正 ・ネットワークおよび仮想コンピューティング環境の分離について、当社内部の管理環境とお客様へ提供している環境も分離している旨を追加 ・装置の処分および再利用について、参照する AWS のウェブページの URL をより望ましいものに修正
2024/01/31	・誤植修正 ・ISO/IEC 27017 の認証取得を反映 ・CISO の役職変更を反映

目次

1. はじめに

1.1. 当ドキュメントの目的

「統合顧客管理（CRM）システム セキュリティに関するホワイトペーパー」をダウンロードいただきありがとうございます。当ドキュメントは「Synergy!（以下、当サービス）」をご利用いただくお客様向けに、運営会社でございますシナジーマーケティング株式会社（以下、当社）の情報セキュリティ体制および契約、機能、運用体制の角度から当サービスのセキュリティ状況をご説明するものです。
また、当ドキュメントには、クラウドセキュリティの認証である「JIP-ISMS517-1.0（ISO/IEC27017:2015）」にて求められている要求事項の中で、特にクラウドサービスの利用者に向けた情報開示が求められている事項につきましても記載させていただいております。該当するものにつきましては、管理策番号を併記しております。

1.2. 当ドキュメントで使用する用語の定義

当ドキュメントで使用する用語につきましては、以下の通り定義しております。

用語	定義
当社	シナジーマーケティング株式会社
当サービス	統合顧客管理（CRM）システム Synergy!
お客様	当サービスを利用されるご契約者
顧客	当サービスを使ってお客様がサービスを提供する対象
DB 格納情報	当サービスの顧客データベースに格納されたデータ

1.3. 当ドキュメントの適用範囲

当ドキュメントの適用範囲は当サービスとなります。

1.4. 当ドキュメントの変更

当ドキュメントの内容は予告なく変更されることがございます。

1.5. 情報セキュリティ要求事項の分析および仕様化

[ISO/IEC27017 14.1.1]
当社が実施しているセキュリティ管理策に関しては当ドキュメントをご参照ください。また、当サービスで提供しているセキュリティ機能に関しては製品資料をご参照ください。

2. 当社のセキュリティ

2.1. 企業概要

2.1.1. 事業概要

当社は「CRM 領域におけるクラウドサービス事業およびエージェント事業」を事業概要とし、以下の 3 つの事業を行っております。

- CRM 関連製品ならびにサービスの企画・ソフト開発・提供
- CRM 戦略構築支援ならびに各種 CRM 業務の代行
- 広告、宣伝に関する企画、制作および広告代理店業

2.1.2. 設立年

創業は 2000 年 9 月となります。

2.1.3. 資本金

2023 年 1 月 1 日現在、90 百万円となります。

2.1.4. 親会社

当社の親会社はペイフォワード株式会社であり、出資比率は 100%となります。なお、2014 年 10 月から 2019 年 7 月までの間は、ヤフー株式会社（現・LINE ヤフー株式会社）が親会社であり、当時の出資比率は 100%でございました。

2.1.5. 本社所在地

[ISO/IEC27017 6.1.3]
当社は大阪本社および東京本社の 2 本社制を採用しており、地理的所在地は以下の通りとなります。

- 大阪本社
  〒530-0003 大阪府大阪市北区堂島 1-6-20 堂島アバンザ 21 階
- 東京本社
  〒102-0083 東京都千代田区麹町 6-6-2 番町麹町ビルディング 5 階 WeWork 麹町

2.1.6. 管轄官庁

当社は届出電気通信事業者であり、管轄官庁は総務省となります。届出番号は「E-12-01633」です。

2.1.7. 従業員数

2023 年 1 月 1 日現在、正社員および契約社員、アルバイトを含めまして 256 名となります。なお、雇用形態別の従業員数や比率は非開示とさせていただきます。

2.1.8. 国家資格保有者数

情報処理技術者試験の資格保有者数は非開示とさせていただきます。

2.2. 外部認証

2.2.1. プライバシーマーク制度

当社は 2004 年 4 月 20 日に「プライバシーマーク制度」に適合している企業として認証を受けており、以降 10 回の更新を続けております。

認証番号	20000604(10)
指定審査機関	一般財団法人関西情報センター(KIIS)
有効期限	2024 年 4 月 19 日

2.2.2. 情報セキュリティマネジメントシステム(ISMS)適合性評価制度

当社は 2020 年 1 月 22 日に「情報セキュリティマネジメントシステム(ISMS)」に適合している企業として認証を受けております。

認証基準	JIS Q 27001:2014(ISO/IEC 27001:2013)
認証登録番号	IS 718028
認証機関	BSI グループジャパン株式会社
有効期限	2025 年 10 月 31 日

2.2.3. ISMS クラウドセキュリティ認証制度

当サービスは 2024 年 1 月 16 日に「ISMS クラウドセキュリティ認証制度」に適合しているクラウドサービスとして認

証を受けております。

認証基準	ISO/IEC 27017:2015
認証登録番号	CLOUD 794651
認証機関	BSI グループジャパン株式会社
有効期限	2025 年 10 月 31 日

2.2.4. 内部監査

情報セキュリティマネジメントシステム（ISMS）およびプライバシーマーク制度の要求に則り、年 1 回情報セキュリティおよび個人情報の取り扱い状況の内部監査を実施し、各種安全管理処置の妥当性の確認、個人情報の取り扱いの妥当性の確認および是正処置を行っております。内部監査はコーポレート部情報システムセキュリティグループにて行っており、監査責任者は同グループマネージャーとなりますが、氏名は非開示とさせていただきます。
内部監査後は内部監査報告書を作成し、経営陣に報告しております。また、是正が必要な指摘事項が発生した場合は、関係部署にて是正計画を作成の上で対応致します。
なお、いわゆるシステム監査は実施しておりません。

2.2.5. 外部監査

外部の監査機関による監査は受けておりません。従いまして、SOC2 および SOC3 レポートはございません。

2.3. 情報セキュリティに関する規定

2.3.1. 情報セキュリティ基本規程

当社では情報セキュリティの基本規定として「情報セキュリティ基本規程」を定めております。またその下位の基本規定として「情報管理規則」「情報セキュリティに関する設備等に関する規則」「情報セキュリティ安全管理措置基準」を定めており、それらを補完する形で細則およびマニュアルを制定しております。
これらの規定類は社内の掲示板に掲示し、従業員に周知しております。

2.3.2. 情報区分程

当社では取り使う情報の機密性を鑑み、次の 5 つに分類して取り扱いを定めております。

情報区分	考え方
極秘	● 漏えいした場合、安全管理措置が有効でなくなる情報 ● 漏えいした場合、情報主体にプライバシー侵害／差別・名誉毀損などを誘発し、かつ悪

	影響範囲が未知数（将来等も含む・影響が当人に限らないなど）な個人情報のうち、元の情報の交換や変更が不可能または困難なもの ● 漏えいした場合、お客様やお客様のエンドユーザー様に経済的損失が生じる情報
秘密	● 漏えいした場合、お客様やお客様のエンドユーザー様にプライバシー侵害／差別・名誉毀損などの被害が生じる情報 ● 漏えいした場合、法令やガイドラインの遵守、契約の履行に支障が生じる情報
限定	● 漏えいした場合、お客様やお客様のエンドユーザー様、従業者個人やその家族に影響する情報 ● 漏えいした場合、当社の事業運営および業務遂行、営業活動に影響する情報
社外秘	● 極秘、秘密、限定、公開以外の情報
公開	● 公開した情報

情報区分は「情報管理規則」にて定義しており、また、具体的にどのような情報がどの情報区分に該当するかを示した「情報区分早見マニュアル」を作成しております。

なお、当サービスに関する情報は次のような情報区分となります。

情報区分	当サービスにおける情報の例
極秘	該当なし
秘密	お客様の顧客データベース
限定	クライアント証明書、お客様の顧客データベースの匿名加工情報
社外秘	ご契約企業の担当者様情報、お客様の顧客データベースの統計情報、ソースコード
公開	一般公開されたお客様のコンテンツデータ、サービス仕様

2.3.3. 規定類の更新

各種規定は必要に応じて更新を行っております。基本規定の更新には、役員会の承認が必要となります。細則およびマニュアルの更新には、当該ドキュメントを主管する部署の部門長の承認が必要となります。

2.3.4. CISO の設置

CISO（Chief Information Security Officer）を設置しており、代表取締役社長・奥平博史が兼任しております。

2.3.5. 情報セキュリティ委員会の設置

情報セキュリティの統括組織として情報セキュリティ委員会を設置しております。委員会のメンバーは CISO を委員長とし、メンバーは原則、代表取締役以外の役員ならびに各部門長となります。また、コーポレート部情報システムセキュリティグループが情報セキュリティ委員会の事務局を務めます。

情報セキュリティ委員会はインシデント対応組織および事故管理組織としても位置づけられ、月 1 回、委員会を開催しております。

2.3.6. 情報セキュリティ部門の設置

CSIRT 等、情報セキュリティの専門部署は設置しておりません。

2.3.7. 情報セキュリティ体制図

当社の情報セキュリティ体制を示す図として「情報セキュリティ体制（図）」を、各種情報セキュリティの役割と担当する組織および責任者を示す表として「情報セキュリティ体制（役割）」を作成しております。なお、責任者の異動や社内組織の変更が発生した場合は、速やかに更新しております。

2.3.8. 情報セキュリティの見直し

CISO および CISO より招集されたメンバーにより、年 1 回、本年度の情報セキュリティの振り返りおよび次年度以降の情報セキュリティに関する取り組みの見直しを行っております。

2.3.9. 情報資産台帳の整備と棚卸し

情報資産台帳を整備し、上期および下期の年 2 回、棚卸しを行っております。なお、台帳は情報区分が秘密以上のものと限定以下のものに分けて整備しております。

2.3.10. ISMS（情報セキュリティ）基本方針の策定と公開

当社では ISMS（情報セキュリティ）基本方針を策定し、コーポレートサイトにて公開しております。
https://corp.synergy-marketing.co.jp/privacy#security

2.4. 個人情報保護体制

2.4.1. 個人情報保護規程

当社では「個人情報保護規程」を定め、個人情報保護マネジメントシステムの運用を行っております。個人情報保護規程は社内の掲示板に掲示し、従業員に周知しております。

2.4.2. 個人情報保護管理者の設置

個人情報保護管理者として、コーポレート部部長を任命しております。なお、氏名は非開示とさせていただきます。

2.4.3. 個人情報教育担当者の設置

個人情報教育担当者として、コーポレート部情報システムセキュリティグループを任命しております。

2.4.4. 個人情報管理台帳の整備と棚卸し

個人情報管理台帳を整備し、上期および下期の年 2 回、棚卸しを行っております。

2.4.5. プライバシーポリシーの策定と公開

当社ではプライバシーポリシーを策定し、コーポレートサイトにて公開しております。
https://corp.synergy-marketing.co.jp/privacy

2.4.6. 個人情報開示等請求

個人情報の利用目的の通知および開示、内容の訂正および追加または削除、利用停止、消去および第三者への停止ならびに保有個人データの第三者提供記録の開示の請求につきましては、適切に対応致します。なお、当社コーポレートサイトにて所定の請求書を公開しております。
https://corp.synergy-marketing.co.jp/privacy#disclosure

2.5. オフィス

2.5.1. フロア定義

大阪本社および東京本社では、次のようなフロア定義となっております。

大阪本社	来客エリア	エントランス、待ち合い、来客用会議室
	就業エリア	執務室、社内会議室、倉庫、休憩エリア
	セキュリティエリア	セキュリティエリア
東京本社	就業エリア	執務室、社内会議室

外来者の方に入室いただけるのは、原則、来客エリアまでとなります。就業エリアおよびセキュリティエリアに入室される場合は、後述の通り、当社従業員が同行の上でゲストカードのストラップの着用が必要です。

2.5.2. 開発および保守業務を行う執務室

当サービスの開発および保守業務は就業エリア内の執務室にて行います。執務室は開発および保守業務を行う従業員以外に、全ての従業員が入室可能です。また、座席はフリーアドレス制を導入しており、開発業務を行う従業員や保守業務を行う従業員、および営業など他の業務を行う従業員と区画分けは行っておりません。
執務室への入室に際して、持ち物検査は行っておりません。スマートフォンやデジタルカメラといった機器の持ち込みも制限しておりません。

2.5.3. 個人情報を取り扱う代行業務を行う執務室

個別の契約となりますが、お客様よりお客様の顧客の個人情報を取り扱う業務を受託した場合は、セキュリティエリアにて業務を行います。セキュリティエリアは原則、同室内にて業務を行う従業員が入室可能です。打ち合わせ等の理由で他の従業員が入室する場合は、紙による入退室記録を取っております。
セキュリティエリアでの業務に際しては、スマートフォンやデジタルカメラといった機器の持ち込みを禁止しており、入室時に各個人のロッカーに保管することを義務付けております。

2.5.4. 入退室管理の実施および記録

「情報セキュリティに関する設備等に関する規則」に基づき、執務室のドアは電子錠により施錠しており、従業員に貸与している IC カードにより解錠致します。入室および退室の記録は 1 年間保存しております。
セキュリティエリアのドアも同様に IC カードにより解錠が可能ですが、同室内にて業務を行う従業員にのみ入室権限を与えております。また、セキュリティエリアのドアにはアンチパスバックを設定しており、入室記録のない IC カードによる退室は行えません。セキュリティエリアの入室および退室の記録も 1 年間保存しております。

2.5.5. 監視カメラ

大阪本社、東京本社共に監視カメラを設置しております。

大阪本社	ドーム型扉開閉時録画	執務室ドア前
	ドーム型 24 時間録画	来客エリア
		サーバールーム
	全方位型 24 時間録画	セキュリティエリア
東京本社	ドーム型 24 時間録画	執務室ドア前

なお、録画データは 90 日間保存しております。

2.5.6. 社員証

執務室およびセキュリティエリア内では、ネックストラップを付けた顔写真付き社員証の着用を義務づけております。また、ネックストラップは正社員および派遣社員、契約社員で色分けしております。出社当日に社員証を忘れた場合は、コーポレート部総務労務グループにてビジターカードを貸与致します。

2.5.7. 従業員以外の執務室への入室

従業員以外のゲストが執務室に入室される場合は、ネックストラップを付けたゲストカードを着用の上、当社従業員が同行して入室いただきます。その際、入室記録などは取得しておりません。
セキュリティエリアに入室される場合も同様ですが、入室に際しては紙による入退室記録を取得しております。

2.5.8. 離席時の対応

離席時におきましては、クリアスクリーンおよびクリアデスクの対応を「情報セキュリティマニュアル」にて定めております。

2.6. 業務端末

2.6.1. 開発および保守業務を行う業務端末

開発および保守業務は、当社より貸与した業務 PC にて行います。業務 PC にはシングルサインオン用のクライアント証明書がインストールされており、メール、スケジュール、ビジネスチャットツールといった業務ツールには、当該クライアント証明書をインストールした業務 PC からのみアクセスが可能です。シングルサインオンの製品名につきましては、非開示とさせていただきます。
業務 PC にはクライアント運用管理ソフトウェアをインストールしており、大阪本社および東京本社の社内ネットワークに接続するには、当該ソフトウェアがインストールされている必要がございます。クライアント運用管理ソフトウェアの製品名につきましては、非開示とさせていただきます。
ノート型の業務 PC につきましては、帰宅時に施錠可能なロッカーに格納することを義務づけております。なお、当社ではテレワークを導入しており、業務 PC の社外への持ち出しは制限しておりませんが、後述の通りストレージの暗号化を行っております。

2.6.2. 個人情報を取り扱う代行業務を行う業務端末

個別の契約となりますが、お客様よりお客様のエンドユーザー様の個人情報を取り扱う業務を受託した場合は、セキュリティエリア内にある専用の業務 PC にて業務を行います。当該業務 PC は、セキュリティエリア内の専用のネットワークに接続されております。当該ネットワークからは、当該ネットワークからしか接続できない専用のファイルサーバにアクセスが可能であり、必要に応じて個人情報を含むファイルの保存を行っております。

2.6.3. ソフトウェアのインストール

業務 PC へのソフトウェアのインストールにつきましては、業務に必要であること、また、ライセンスを遵守することなどルールを定めておりますが、インストール権限は各従業員に渡しており、制限は行っておりません。ただし、業務 PC にはクライアント運用管理ソフトウェアを導入しており、各従業員がインストールしたソフトウェアは把握しております。
なお、セキュリティエリア内の専用の業務 PC につきましては、管理者以外によるソフトウェアのインストールは行えません。

2.6.4. ウイルス対策ソフトの導入

業務 PC には次世代型のウイルス対策ソフトを導入しております。これは AI による学習を通し、PC 内の挙動を監視することで、パターンファイルによって駆除する従来型のウイルス対策ソフトのみでは対応できなかった脅威からも PC を保護するものです。なお、ソフトウェアの名称は非開示とさせていただきます。
パターンファイルは自動にて更新しており、また週 1 回のフルスキャンを行っております。

2.6.5. OS のアップデート

業務 PC の OS にアップデートが発生した場合は、コーポレート部情報システムセキュリティグループにて動作を確認の上、期日を定めて全利用者に OS のアップデートを求めております。アップデートの状況は把握しており、期日までに対応が行えていない場合は、コーポレート部情報システムセキュリティグループより対応を指示致します。なお、社用携帯につきましては、OS のアップデートは利用者の判断となります。

2.6.6. EDR の導入

業務 PC には EDR（Endpoint Detection and Response）製品を導入しております。これは万が一業務 PC が外部からハッキングなどの攻撃やデータの盗難に遭った場合であっても、その脅威を速やかに検知できるよう監視するものです。
EDR は外部の契約業者により 24 時間 365 日監視しております。なお、当該契約業者に対しては年 1 回の委託先監査を実施し、当社と同等かそれ以上の情報セキュリティ体制であることを確認しております。EDR の製品名および契約業者名は非開示とさせていただきます。

2.6.7. ストレージの暗号化

業務 PC のストレージは暗号化しており、OS へのログインとは別に、起動時にパスワードを入力する必要がございます。

2.6.8. 外部記憶媒体の接続

業務 PC にはクライアント運用管理ソフトウェアをインストールしており、許可されていない外部記憶媒体は認識しないよう制御しております。なお、業務上、外部記憶媒体を利用する必要がある場合は、申請の上で認証済み外部記憶媒体の貸し出しを行います。これには USB メモリ、外付けハードディスク、CD/DVD-R ドライブ、メモリーカードリーダーが含まれます。

2.6.9. パスワード管理

業務 PC および業務システムのパスワードにつきましては、「アクセス権限管理細則」にてパスワードポリシーを策定しております。パスワードは次の条件を満たす必要がございます。

- 第三者が容易に推測できない文字列を使用すること
- 8 文字以上の長さにすること
- 下記 4 つのグループから最低 3 グループを使用すること
  - 英字の大文字
  - 英字の小文字
  - 数字
  - 特殊記号

なお、パスワードの定期的な変更は、総務省通達を鑑みて義務づけておりません。

2.6.10. ログの取得

業務 PC にはクライアント運用管理ソフトウェアをインストールしており、アクセスログ、操作ログなどを取得しております。具体的に取得しているログの種類は非開示とさせていただきますが、各種ログは 1 年間保存しております。

2.6.11. スクリーンロック

業務 PC は無操作の場合、10 分後にスクリーンロックされるよう設定しております。

2.6.12. 社用携帯

社用携帯から社内ネットワークへのアクセスは行えません。
社用クラウドサービスにつきましては、クライアント証明書を用いたシングルサインオン認証を行うことで、メール、スケジュール、ビジネスチャットツールといった業務ツールにアクセスが可能となります。
また、紛失時の対応として、位置情報の取得およびリモートワイプの設定を行っております。

2.7. テレワーク

2.7.1. テレワークの種類

当社では次の形態によるテレワークを実施しております。

- 在宅勤務
- モバイル勤務

なお、テレワークの実施にあたっては、個別にお客様の承諾は得ておりません。

2.7.2. テレワークに関する規定

テレワークの定義やテレワークにて実施可能な業務については、「テレワーク管理細則」に定めております。また、「テレワークにおけるセキュリティガイドライン」にてテレワーク実施における注意事項を定めて周知しております。

2.7.3. 在宅勤務

当社において在宅勤務とは、自宅及び自宅に準ずる場所で業務を行うことを言います。自宅に準ずる場所とは、従業員ならびに配偶者の実家、親族宅などを言い、知人宅などは含めません。
在宅勤務においてインターネットに接続する必要がある場合は、自宅等で契約しているプロバイダもしくはモバイル Wi-Fi ルーター、社用携帯によるテザリング、会社貸与のモバイル Wi-Fi ルーターのいずれかを使用する必要がございます。

2.7.4. モバイル勤務

当社においてモバイル勤務とは、顧客先、カフェ、ホテルなど当社事業拠点以外の場所や移動中の交通機関等で業務を行うことを言います。
モバイル勤務においてインターネットに接続する必要がある場合は、自宅等で契約しているモバイル Wi-Fi ルーター、社用携帯によるテザリング、会社貸与のモバイル Wi-Fi ルーターのいずれかを使用する必要がございます。

2.7.5. テレワークにおける禁止事項

個人情報を取り扱う業務につきましては、テレワークでの実施を認めておらず、当社オフィス内で業務を行うことを定めております。また情報の種類に関わらず、情報区分が「秘密」以上に該当する場合も当社オフィス内で業務を行うことを定めております。
具体的には次のような業務について禁止もしくは制限しております。

業務例	在宅勤務	モバイル勤務（個室）	モバイル勤務
当サービスの開発業務	○	○	○
顧客データベースを扱う保守業務	×	×	×
顧客データベースを扱わない保守業務	○	○	○
電話によるお客様のサポート対応	○	×	×
お客様の個人情報を取り扱う代行業務	×	×	×
個人情報を問わず情報区分が秘密となる情報を扱う業務	×	×	×
個人情報を問わず情報区分が限定となる情報を扱う業務	○	○	×
個人情報を問わず情報区分が社外秘となる情報を扱う業務	○	○	○
Google Meet や Zoom を使ったテレビ会議	○	○	×

2.8. 事故および災害対応体制

2.8.1. 情報漏えい事故時対応ガイドライン

当社では、情報漏えいなど万が一の重大インシデント発生時した場合、速やかに対策本部を立ち上げて全社的に対応ができるよう、「情報漏えい等事故時対応ガイドライン」を定めております。

2.8.2. 影響度の判定

インシデント発生時は「判定基準表」に基づき影響度を判定致します。影響度は S、A、B、C の 4 つのランクに区分しております。

ランク	インシデントの影響度合い
S ランク	データの漏えい、減失、毀損に影響がある
A ランク	データの漏えい、減失、毀損に影響はないが、サービス提供に重大な影響を及ぼしている
B ランク	データの漏えい、減失、毀損に影響はないが、サービス提供に軽微な影響を及ぼしている
C ランク	影響度の低いリンク設定ミス、誤表記など

2.8.3. インシデントの管理

インシデントが発生した場合は「事故報告システム」にインシデント内容を登録し、恒久対策が完了するまでの経過を管理しております。また、発生した全てのインシデントは情報セキュリティ委員会において報告致します。
事故報告システムは社内に公開されており、同種の事故防止のための社内情報共有も兼ねております。

2.8.4. 対策本部の設置

重大なインシデントや広範囲に影響があるインシデントの場合は必要に応じて、情報漏えい等事故時対応ガイドラインに則って、代表取締役社長を対策本部長とする対策本部を立ち上げます。対策本部のメンバーは常勤の取締役および各部門長となります。
従いまして、常設のインシデント対応部署はございません。

2.8.5. お客様への連絡

お客様への通知は、以下のいずれかの手段により実施致します。

a. 当サービスの管理画面内に掲示
b. 当サービスのサポートページに記載
c. 当サービスのシステム管理担当者として登録されているアドレス宛にメールにて
d. 当社営業担当もしくはカスタマーサポートより個別に電話またはメールにて

お客様への連絡を担当する部署につきましては、あらかじめ「情報漏えい等事故対応ガイドライン」にて定めております。

2.8.6. 監督省庁および関係機関への連絡

個人情報の漏えい、滅失、毀損に影響のあるインシデントおよび電気通信事業に関するインシデントの場合は、管轄官庁である総務省および個人情報保護委員会への報告を行います。また、関係機関として、プライバシーマーク制度および情報セキュリティマネジメントシステム（ISMS）の審査機関にも報告致します。
関係省庁への連絡を担当する部署につきましては、あらかじめ情報漏えい等事故対応ガイドラインにて定めております。また、報告の手順は「関係省庁報告マニュアル」にて定めております。

2.8.7. 再発防止策の策定

インシデントが解消された後は、恒久的な再発防止策を策定し、事故報告システムにて報告を行います。また、必要に応じてお客様に報告書を提出致します。インシデントのクローズには、再発防止策を含めて部門長の承認が必要となります。

2.8.8. 社内処分

事象整理、原因分析ののち、「就業規則」に抵触する事実があった場合は処分を行います。

2.8.9. 災害時の対応

天災や火災などの災害発生時に適切な対応が行えるよう、管理体制や基本方針を「災害危機管理基本方針」にて定めております。

2.8.10. 緊急連絡先の整備

全正社員に社用携帯を貸与しております。また、契約社員および派遣社員、アルバイトの一部にも社用携帯を貸与しております。社用携帯の電話番号は社内の掲示板にて確認が可能です。
また、それとは別に全従業員の緊急連絡先を取得しており、年 2 回、更新しております。なお、マネージャー以上の職位の緊急連絡先につきましては、四半期毎に確認し社内掲示板に掲示しております。

2.8.11. BCP（業務継続計画）

BCP につきましては、「事業継続計画マニュアル」を策定しております。

2.9. 従業員の入社および退職

2.9.1. 採用

当社では新卒採用および中途採用を行っております。いずれの場合も本人の才能および能力を鑑みて採用を行っておりますが、採用に際していわゆる身辺調査は行っておりません。

2.9.2. 誓約書

入社時においては雇用形態に関わらず、業務上知り得た秘密情報および顧客の個人情報の取り扱いについて、法令や当社規定の遵守および守秘義務について定めた誓約書を取得しております。また、誓約書の効果は退職後も有効となります。
なお、懲罰につきましては「就業規則」にて定めております。

2.9.3. 入社時研修

雇用形態に関わらず、入社時に情報セキュリティおよび個人情報保護に関する研修を行っております。この研修は集合研修となりますが、昨今の状況を鑑み、講師および受講者ともテレビ会議システムを使ったオンラインミーティング形式となる場合がございます。
研修の内容は、弊社の基本的な情報セキュリティの考え方および個人情報保護の考え方となります。
また、クラウドサービスに関わる部署へ配属される者につきましては、別途クラウドセキュリティ研修を実施致します。

こちらは、e ラーニング形式にて実施し、オンライン研修資料にて受講の上、理解度テストを実施して満点の取得が必須となります。
研修の内容は、講師がその時々によってピックアップして決定しております。

2.9.4. 入社時研修退職時の対応

退職に際しては返却が必要となる貸与物を記した「返却物封筒」を退職者に渡し、最終出社日までに全ての貸与物を返却いただきます。この中には業務 PC および社用携帯、社員証、入室用の IC カードが含まれます。また、退職後速やかに各種システムへのアクセス権を削除しております。

2.10. 定期的な教育

2.10.1. 定期的な教育に関する規定

情報セキュリティに関する教育につきましては「情報セキュリティ基本規程」にて、個人情報保護に関する教育につきましては「個人情報保護規程」にて、定期的に実施することを定めております。

2.10.2. 定期教育

定期研修は年 2 回、前期と後期において行っております。前期は情報セキュリティおよびコンプライアンスをテーマに、後期は情報セキュリティおよび個人情報保護をテーマに、e ラーニング形式にて実施しております。オンライン研修資料にて受講の上、理解度テストを実施し、満点の取得が必須となります。
研修の内容は講師がその時々によってピックアップして決定しております。

また、クラウドサービスに関わる部署につきましては、クラウドセキュリティに関わる教育を定期研修として年2回、前期と後期に行っております。こちらも、e ラーニング形式にて実施し、オンライン研修資料にて受講の上、理解度テストを実施し、満点の取得が必須となります。
研修の内容は講師がその時々によってピックアップして決定しております。

2.10.3. その他

当社にも関係するような他社事故事例を収集し、当社として気をつけるポイントなどをまとめた上で全社周知を行っております。ただし、いわゆるサイバーセキュリティに関する研修は行っておりません。また、訓練に該当するような教育も行っておりません。

2.11. 外部委託

2.11.1. 外部委託について

「Synergy!契約規定」の第 12 条にございます通り、当社は当社の責任により SLA に定められた運用業務の一部または全部を第三者に委託することがございます。委託に際しましては、個別にお客様の承諾は得ておりません。また、委託先や委託内容、委託状況などの詳細は非開示とさせていただきます。
ただし、DB 格納情報などお客様よりお預かりしております個人情報を取り扱う業務の委託は行いません。

2.11.2. 個人情報を取り扱う代行業務における外部委託について

個別の契約となりますが、お客様よりお客様のエンドユーザー様の個人情報を取り扱う業務を当社に委託された際に、当該契約が当社から外部へ一部もしくは全部を委託することが前提の場合は、書面にてお客様から外部委託の承諾を得た上で実施しております。また、委託先につきましては当社の規定に従い委託先監査を行い、当社と同等もしくはそれ以上の情報セキュリティ体制であることを確認しております。

2.12. その他

2.12.1. 監査の受け入れ

お客様もしくはお客様の監督省庁による監査をご希望の場合は、担当営業までご相談ください。文書監査および訪問監査を受け入れております。ただし、監査の内容によってはお受けできない場合もございますので、全ての監査の受け入れをお約束するものではございません。また、監査を受け入れた場合であっても、一部、非開示とさせていただく事項もございます。

3. 当サービスのセキュリティ

3.1. 当サービスのご利用に際して

3.1.1. サービス概要

当サービスはクラウドで提供する CRM システムであり、以下の機能を有しております。

機能	概要
データベース	顧客データ、および顧客に関連するマーケティングデータを登録、更新、削除、閲覧する機能
フォーム	顧客データの登録や変更が可能な Web フォームを作成する機能
メール	顧客にカスタマイズされたメールを配信する機能
API	外部システムから当サービスの以下の機能を利用可能な API 機能 ● 顧客データベースの読み出し・登録・更新・削除などの操作

当サービスには、データの閲覧やフォームを作成するクライアント機能と、クライアント機能より作成した Web フォームであるコンシューマ機能がございます。当サービスのクライアント機能はクライアント証明書をインストールしたブラウザからアクセスしてご利用いただけます。また当サービスのコンシューマ機能にはブラウザからアクセスいただけます。

3.1.2. Synergy!契約規定

「Synergy!契約規定」は、当サービスをご利用いただく上での基本的事項を定めたものとなります。

3.1.3. 責任分界点

[ISO/IEC27017 6.1.1]
当サービスにおける責任分界点は以下の通りとなります。

- 当社の責任範囲
  - アプリケーション開発・保守
  - ミドルウェア/OS/仮想環境
  - 当サービスをウェブ上に公開するためのインターネット接続環境

- お客様の責任範囲
  - インターネット接続環境や端末など当サービスに接続するための環境
  - ID や証明書等ログイン情報やユーザの管理
  - 当サービスの設定

- API を利用したシステム開発・保守
- 当サービスに対してお客様が行ったカスタマイズ

3.1.4. 情報セキュリティの役割および責任

[ISO/IEC27017 CLD.6.3.1]
当社は「Synergy!契約規定」にて当社とお客様それぞれの役割および責任について明記しており、また当ドキュメントの「責任分界点」にて当社とお客様とのセキュリティの責任範囲を定めております。これらにつきましては、当サービスの利用開始時にご同意いただく事項となります。

3.1.5. システムのアップグレード

当サービスでは適宜システムのアップグレードを実施致します。 お客様へはサポートサイト、管理画面からご案内致します。なお、アップグレードに伴う費用負担は発生致しませんが、アップグレードに関わらない費用改定および新たなオプション機能が追加された際に当該オプションを契約いただく場合は、これに該当致しません。

3.1.6. カスタマイズ

EC サイトとの連携やクライアント機能では実装できないカスタマイズなどにつきましては、当社担当営業にご相談ください。

3.2. Amazon Web Service

3.2.1. Amazon Web Service および提供会社

Amazon Web Services（アマゾンウェブサービス、以下、AWS）は Amazon Web Services, Inc（以下、AWS 社）が提供するクラウドコンピューティングサービスです。AWS はクラウドサーバーである Amazon Elastic Compute Cloud （Amazon EC2、以下、EC2）やクラウドストレージの Amazon Simple Storage Service （Amazon S3）、クラウドデータベースの Amazon Relational Database Service（Amazon RDS）、ドメインネームサービス（DNS）の Amazon Route 53 など、さまざまなサービスで構成されております。
当社は日本法人であるアマゾンウェブサービスジャパン合同会社と契約し、当サービスは AWS にホスティングして稼働しております。

3.2.2. データセンターの所在地

[ISO/IEC27017 6.1.3]
当サービスの主データセンターは AWS の「アジアパシフィック（東京） ap-northeast-1（以下、東京リージョン）」と

致します。また、遠隔地バックアップとして、AWS の「アジアパシフィック（大阪） ap-northeast-3（以下、大阪リージョン）」にバックアップデータを保存致します。当サービスでは冗長化のため、各リージョンにおいて複数のアベイラビリティゾーンを使用しております。なお、AWS 社は各リージョンにおけるデータセンターの所在地（都道府県名）を開示しておりません。
従いまして、お客様のデータを保存する可能性のある国は、日本国のみとなります。

3.2.3. 安全性の確認

AWS は次のような外部認証やコンプライアンスプログラムに則って設計・運用・提供されております。

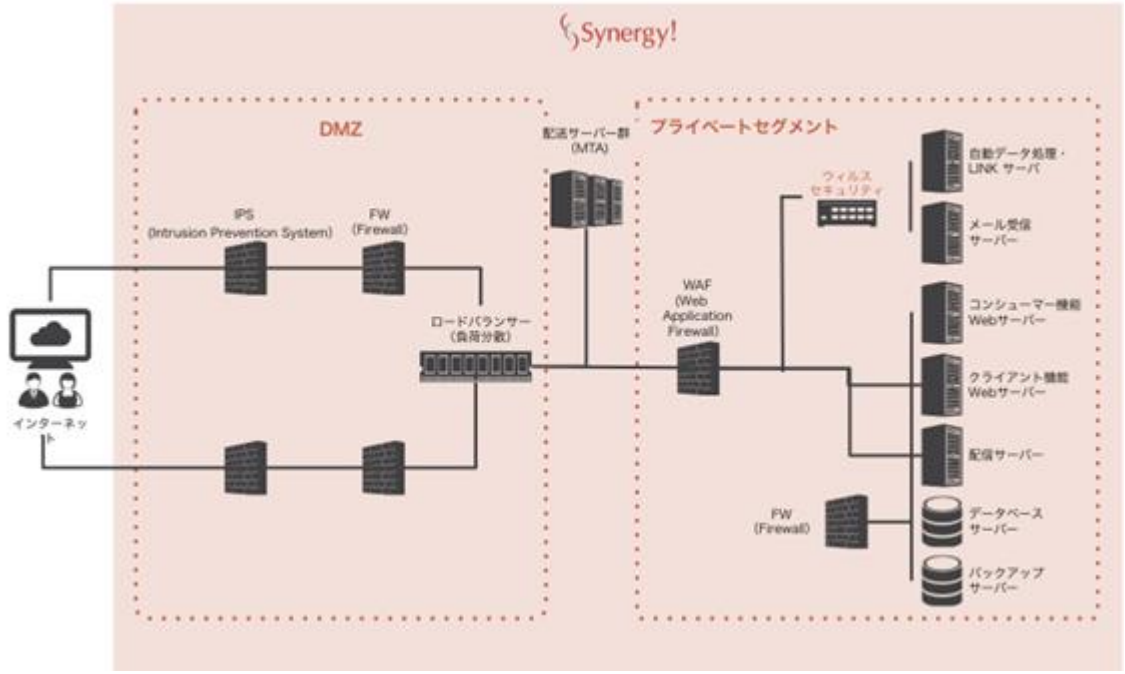
- CSA
- Cyber GRX
- Cyber Vadis
- ISO 9001
- ISO 22301
- ISO 27001
- ISO 27017
- ISO 27701
- ISO 27018
- PCI DSS レベル 1
- SOC 1、SOC 2、SOC 3
- Fin Tech
- FISC
- ISMAP
- 医療情報ガイドライン
- NISC

当社は AWS 社との契約において、AWS 社が当社のデータを取り扱わないことおよび適切にアクセス制御を行っていることから、AWS の利用を委託と考えておりません。しかしながら、個人情報を AWS に保存することから、自社の設備の一部と見なして安全管理措置を取る必要があると考えております。
当社は AWS 社の SOC2 レポートを確認し、監査法人が例外意見を出していないことを確認しております。加えて、NDA を締結した上で AWS 社とミーティングを行い、AWS の安全性を確認しております。

3.3. インフラストラクチャー

3.3.1. 構成図

当サービスのインフラストラクチャーの全体像は次の通りです。データベースをはじめ、サービスを構成する重要なサーバはすべてインターネットから直接アクセス不可能なプライベートセグメントに設置しております。また、インターネットから直接アクセス可能な箇所には DMZ を設け、必要最小限のサーバのみを設置しております。



3.3.2. ファイアウォール

当サービスではファイアウォールを導入し、不正アクセスや侵入などの脅威を回避しております。なお、ファイアウォールの製品名や設定・運用のポリシーは非開示とさせていただきますが、適切に運用しております。

3.3.3. IPS

当サービスでは IPS を導入し、外部の脅威より攻撃を受けたとしても、その攻撃内容を検知し遮断致します。なお、製品名や設定・運用のポリシーなどの詳細は非開示とさせていただきますが、適切に運用しております。

3.3.4. WAF

当サービスでは WAF を導入し、ファイアウォールや IPS では防御しきれない Web アプリケーションのぜい弱性を利用した攻撃をブロックしております。なお、WAF の製品名や設定・運用のポリシーなどの詳細は非開示とさせていただきますが、適切に運用しております。

3.3.5. DDoS 対策

DDoS 対策と致しまして、当サービスでは AWS にて提供されております DDoS 対策システムを導入しております。

なお、製品名や設定・運用のポリシーなどの詳細は非開示とさせていただきますが、適切に運用しております。

3.3.6. 障害対策

当サービスを構成するネットワークおよびサーバは複数台で構成しており、単一障害点はございません。これらの機器に故障が生じた場合においても、当サービスの継続または早期復旧を可能としております。特にストレージに関しましては、同一データを複数のストレージへ同時に書き込むことによりデータの損失を防いでおります。

3.3.7. バックアップ

[ISO/IEC27017 12. 3. 1]
データベースにつきましては、直近 1 週間までロールバック可能なリアルタイムのバックアップを当サービスの主データセンターである AWS の東京リージョンにバックアップしております。また、遠隔地バックアップとして、AWS の大阪リージョンにもバックアップしております。
また、これらのバックアップは障害対策を目的としており、お客さまのご要望による個別復旧には対応致しかねますが、お客様にて管理画面より顧客データベースのデータをエクスポートすることも可能です。
ファイル管理機能にてアップロードされたファイルにつきましては、バックアップの対象ではございませんが、AWS の堅牢なシステムによって保護されております。

3.3.8. 暗号化

Web ブラウザとシステム間の通信を暗号化しております。暗号化通信のバージョンは TLS1.2 もしくは 1.3 となります。
レスポンスの重視および部分検索機能の提供からデータは暗号化して保存しておりませんが、データベースサーバのストレージの暗号化は実施しております。

3.3.9. 暗号化機能に対する規制

[ISO/IEC27017 18.1.5]
当サービスでは、輸出規制の対象となる暗号化技術は採用しておりません。

3.3.10. ネットワークおよび仮想コンピューティング環境の分離

[ISO/IEC27017 13.1.3] [ISO/IEC27017 CLD.9.5.1]
ネットワーク及び仮想コンピューティング環境につきましては、本サービスではお客様が別のお客様のデータを閲覧することができないよう適切に分離しており、当社内部の管理環境とお客様へ提供している環境も分離しております。
また、データベースにつきましては、ご契約単位でデータベーススキーマを分けており、テナント間でデータの隔離を行っております。

3.3.11. 仮想マシンの要塞化

[ISO/IEC27017 CLD.9.5.2]
当サービスでは、仮想マシンの要塞化を以下の事項により実施しております。

- データベースをはじめ、サービスを構成する重要なサーバーはすべてインターネットから直接アクセス不可能なプライベートセグメントに設置しております。
- セキュリティに関する更新が公開された場合、是非を検討の上必要に応じて通常 1 ヶ月以内に当サービスへセキュリティパッチを適用しております。
- 外部から EC2 へのアクセスは AWS Session Manager に限定し、アクセスログを取得しています。
- 必要最低限のポートのみを解放しております。

3.3.12. ウイルス対策

当サービスでは、外部よりメールやファイルを受信する機能を有するサーバにはウイルス対策ソフトを導入しております。ウイルスゲートウェイおよびアンチウィルス対策ソフトにより、ファイルに含まれる脅威からサーバを防御致します。なお、パターンファイルは自動更新とし、常に最新状態を保っております。

3.3.13. OS のアップデート

セキュリティに関する更新が公開された場合は是非を検討の上、必要に応じて通常 1 ヶ月以内に当サービスへ適用致します。また、JVN のぜい弱性情報を定期的に確認しております。

3.3.14. セキュリティパッチ

セキュリティに関する更新が公開された場合は是非を検討の上、必要に応じて通常 1 ヶ月以内に当サービスへ適用致します。また、JVN のぜい弱性情報を定期的に確認しております。

3.3.15. EOL を迎えた製品の利用

極一部のアプリケーションプログラムにおいて、影響度およびリスク等を勘案した上で、EOL を迎えた製品を利用しております。なお、データベースやネットワーク機器につきましては、EOL を迎えた製品の利用はございません。

3.3.16. 装置の処分および再利用

[ISO/IEC27017 11.2.7]
当サービスは AWS を使用しておりますが、AWS ではデバイスの設置、修理および最終的に不要になった場合の破

棄について厳格な基準が設けられており、それに基づいて対応が行われます。
https://aws.amazon.com/jp/compliance/data-center/controls/

また、AWS へのアクセスなど運用および保守に利用しているサーバ機器（VDI）につきましては、処分の際はストレージの破壊処理もしくは粉砕処理を行い、破棄証明を取得致します。なお、再利用は行いません。

3.3.17. クロックの同期

[ISO/IEC27017 12.4.4]
当サービスにおけるクロックの同期には、AWS が提供する NTP サービスを採用しております。なお、当サービス内で提供する時刻情報は、日本標準時（JST）にて取得致します。

3.3.18. 処理性能

当サービスにおける各処理の応答時間は定めておらず、ベストエフォートとなります。また、同時接続利用者数もベストエフォートとなります。

3.4. クライアント機能のセキュリティ

3.4.1. クライアント機能

当サービスのデータベースやフォームは、クライアント機能の管理画面を通して操作が可能となります。

3.4.2. クライアント機能へのアクセス

[ISO/IEC27017 9.2.3]
お客様が管理画面にアクセスされる際は、ユーザ ID およびパスワードの入力に加えて、お客様からお申し出がない限り、ご契約単位で発行されるクライアント証明書（デジタル証明書）が操作される PC にインストールされている必要がございます。また、IP アドレスによるアクセス制限もオプションにて提供しております。
なお、通信は TLS1.2 もしくは TLS1.3 にて暗号化されております。

3.4.3. パスワードポリシーの設定

管理画面にログインするためのアカウントのパスワードにつきましては、お客様のポリシーに合わせて以下の任意の内容の設定を行っていただけます。

- 初回ログイン時にパスワードの再設定の有無

- パスワードの有効期限(30～365 日もしくは無制限)
- パスワードで使用する文字種の強制(半角英字(小文字)、半角英字(大文字)、半角数字、半角記号)
- パスワードの文字数(8～30 文字)

3.4.4. アカウントロック

管理画面にログインするためのアカウントにつきましては、お客様のポリシーに合わせて認証失敗によるアカウントロックの設定を行っていただけます。

- アカウントロックを行わない
- 設定した回数(3～9 回)の認証失敗にてアカウントをロックする

3.4.5. 強制的なログアウト

管理画面にログインしているユーザのうち、指定したユーザーの強制的なログアウトを行っていただけます。これにより、ユーザが意図しない操作を行っている場合などに、管理者の権限による強制的な操作の中断が可能となります。クライアント機能におけるセッションタイムアウトは 3 時間となります。また、同一ユーザのログイン情報使用した同時ログイン(多重ログイン)を禁止しております。

3.4.6. パスワードの暗号化

[ISO/IEC27017 10.1.1]
クライアント機能の管理画面にログインするためのパスワードは、bcrypt によってハッシュ化されております。

3.4.7. クライアント機能のログ

[ISO/IEC27017 12.4.1][ISO/IEC27017 CLD 12.4.5]
当サービスでは、クライアント機能の管理画面で行われた操作のログを全て保存しております。操作ログには以下の項目を保存しております。

- 操作日時
- 操作ユーザ名
- 操作ユーザの権限グループ
- 操作元の IP アドレス
- 操作内容

操作ログは管理画面より閲覧可能であり、解約されるまでの間、全ての操作ログを保存致します。これにより、お客様にてユーザの不正利用の発見が可能となります。

3.4.8. ユーザの登録および削除

[ISO/IEC27017 9.2.1]
管理者アカウントにつきましては、お申し込み時にご申請いただきました管理者メールアドレスにて発行致します。初期パスワードは当システムが発行したものをメールにて通知致しますが、初回ログイン時に変更をお願いしております。
管理者以外のユーザにつきましては、管理者アカウントにて管理画面にログインいただいた後、「共通設定」の「ユーザ管理」より新規登録を行ってください。また、ユーザの削除も「ユーザ管理」のユーザ一覧画面にて行っていただけます。
詳しくは、下記サポートサイトをご確認ください。

- ユーザを新規登録する
  https://support.crmstyle.com/security/security-1395
- ユーザを削除する
  https://support.crmstyle.com/security/security-1407

3.4.9. ユーザのアクセス権限設定

[ISO/IEC27017 9.2.2]
クライアント機能では、ユーザの操作可能機能を詳細に設定することができ、社内スタッフの役割および責任に応じた権限設定が可能となります。顧客データベースにつきましては、行レベルでのアクセス制限機能は提供しておりませんが、個人情報のフラグを立てたデータベース項目につきましては、アクセス可能なユーザを制限していただけます。

3.4.10. ユーザの秘密認証情報の管理

[ISO/IEC27017 9.2.4]
管理者の初期パスワードはメールにてお知らせしております。また、パスワードはログイン後に管理画面にて変更していただけます。
ユーザの初期パスワードは管理者を含め、ユーザ管理の権限を有しているユーザであれば、管理画面よりユーザ作成時に設定が可能となります。また、設定済みのパスワードの変更も可能となります。

3.4.11. 情報へのアクセス制限

[ISO/IEC27017 9.4.1]
当サービス内の各機能へのアクセス権および顧客データベースへのアクセス権は、ユーザ管理権限を有するユーザであれば、管理画面にて各ユーザ単位に設定が可能となります。
設定可能な権限につきましては、下記サポートサイトをご確認ください。

- 権限項目一覧
  https://support.crmstyle.com/security/security-1380

3.4.12. 情報のラベル付け

[ISO/IEC27017 8.2.2]
当サービスのデータベース設計において各項目にラベル付けを行われる場合は、「管理用メモ」をご利用いただけます。また、メール配信につきましては、フォルダを作成して作成したメールの管理を行っていただけます。

3.4.13. 顧客データベースのデータの削除

[ISO/IEC27017 CLD.8.1.5]
お預かりした以下のデータにつきましては、ご解約の翌月 7 日に自動的に消去致します。また、その 7 日後にはバックアップからも完全に消去されます。 なお、解約時にお客様にて顧客データベースのデータを削除いただいた場合は、その時点で消去が行われ、その 7 日後にはバックアップデータからも完全に消去されます。

- お客様の顧客データベースの顧客データ
- 管理画面におけるお客様のユーザ情報
- 操作ログ

なお、当社によるお客さまへのデータの返却は実施しておりません。解約完了日までにお客さまご自身にて管理機能よりデータをエクスポートしてください。また、消去は物理データ削除にて行いますが、ご解約に際してデータベースサーバのストレージの初期化は行っておりません。

3.4.14. お客様が実行可能な重要操作について

[ISO/IEC27017 CLD.12.1.5]
当サービスにおいてお客様が実施可能である重要操作に関しては、以下の手順書をご用意しております。

- 顧客データ一括削除
  https://support.crmstyle.com/db/db-masterdeletion
- 履歴データ一括削除
  https://support.crmstyle.com/db/db-historydeletion
- データ一括操作について
  https://support.crmstyle.com/db/db-bulkoperation

3.5. コンシューマ機能のセキュリティ

3.5.1. コンシューマ機能

当サービスには、顧客が会員登録や資料請求をするための Web フォームを作成するフォーム機能がございます。コンシューマ機能とは、フォーム機能を用いて作成した Web フォームを指します。フォームから入力されたデータは、自動的に当サービスのデータベースに書き込まれます。新しい顧客を登録する「新規フォーム」や既存顧客のデータを更新する「変更フォーム」を作成していただけます。

3.5.2. コンシューマ機能へのアクセス

コンシューマ機能の変更フォームでは、変更対象の顧客を認証する機能がございます。認証においては複数の認証項目を設定することが可能となっております。

3.5.3. パスワードポリシーの設定

コンシューマ機能の認証項目にパスワードハッシュ型を指定した場合は、パスワードの文字数やパスワードの強度の設定が可能となっております。

3.5.4. パスワードの暗号化

[ISO/IEC27017 10.1.1]
パスワードハッシュ型を使用した場合、パスワードは bcrypt にてハッシュ化した上でデータベースに保存されます。

3.5.5. コンシューマ機能のログ

コンシューマ機能へのアクセスログは 1 年間保存しておりますが、保守を目的に取得しているものであり、お客様には提供しておりません。

3.5.6. 入力データ形式の制限機能

想定外のデータが入力されないよう、フォーム機能を用いて Web フォームを作成する際に、お客様にて文字数や文字種の制限を設定いただけます。

3.5.7. GDPR

当サービスは EU 一般データ保護規則（GDPR）に対応しておりません。

3.5.8. その他

フォーム機能を用いて作成した Web フォームには、アクセス可能な IP アドレスやリファラーによる制限を設定いただけます。また、bot による大量投稿（スパム）などの迷惑行為からサイトを保護するため、Google 社が提供しているスパム防止機能である「reCAPTCHA v3」を設定いただけます。

3.6. メール配信機能のセキュリティ

3.6.1. メール配信機能

メール配信機能におきましては、次の機能をお客様にて選択してご利用いただけます。

- 電子署名を付与してメールを配信する機能
- 送信ドメイン認証の設定を実施していただき、当社の SPF レコードを設定すること

3.7. メンテナンスおよび機能改善リリース

3.7.1. 変更に関する通知

[ISO/IEC27017 12.1.2]
機能の追加および変更や廃止、一時的なメンテナンスなど、お客様に影響を与える可能性がある変更を行う場合は、以下のいずれかの手段により変更に関する通知を行います。

a. 当サービスの管理画面内に掲示
b. 当サービスのサポートページに記載
c. 当サービスのシステム管理担当者として登録されているアドレス宛にメールにて

変更に関する通知には以下の事項を含みます。

- 変更の種類
- 予定日時
- 技術的な説明
- 変更開始及び終了アナウンス

3.7.2. 定期メンテナンス

[ISO/IEC27017 12.1.2]
当サービスの安定稼動や性能向上のために、当サービスの一部または全部を停止してメンテナンス作業を実施することがございます。
定期的なメンテナンスにつきましては、お客様の業務に大きく影響が発生する場合は 2 週間前までに、そうでない場合は1週間前までに通知致します。

1 回のメンテナンス作業における停止時間の合計は、以下を目標と致します。

- クライアント機能で最大 8 時間以内
- コンシューマ機能で最大 4 時間以内

定期メンテナンス作業の日時および作業に伴う停止時間は、サービスへの影響が最小となるように努力致します。また、一部サービスの代替手段についても可能な範囲で検討致します。

3.7.3. 機能改善リリース

[ISO/IEC27017 12.1.2]
当サービスにおけるシステムのアップグレードを行うために、当サービスの一部または全部を停止して機能改善リリースを実施することがございます。
機能改善リリースにつきましては、お客様の業務に大きく影響が発生する場合は 2 週間前までに、そうでない場合は1週間前までに通知致します。

1 回のリリース作業における停止時間の合計は、以下を目標と致します。

- クライアント機能で最大 8 時間以内
- コンシューマ機能で最大 4 時間以内

リリース作業の日時および作業に伴う停止時間は、サービスへの影響が最小となるように努力致します。また、一部サービスの代替手段についても可能な範囲で検討致します。

3.7.4. 計画外のメンテナンス

[ISO/IEC27017 12.1.2]
緊急メンテナンスなど計画外のメンテナンスを実施する場合がございます。お客様の業務に大きく影響が発生する場合は、予定日時等が決まり次第、速やかに通知致します。

3.8. 当サービスの障害および事故

3.8.1. 社内報告制度

当サービスの障害および事故につきましては、検知後に適切な対応をとれるよう、社内に報告制度を設けております。報告後は手順に従い、重要度の判定や必要な場合は対策委員会を設置し、復旧を実施致します。

3.8.2. 連絡方法

[ISO/IEC27017 16.1.1]
障害および事故発生時は、重要度により当社の判断にて通知致します。また、お客様に大きな影響を与える障害および事故（データの消失、長時間のシステム停止等）が発生した場合は、検出してから 72 時間以内を目標に通知致します。
お客様への通知は、以下のいずれかの手段により実施致します。

a. 当サービスの管理画面内に掲示
b. 当サービスのサポートページに記載
c. 当サービスのシステム管理担当者として登録されているアドレス宛にメールにて
d. 当社営業担当もしくはカスタマーサポートより個別に電話またはメールにて

3.8.3. 情報セキュリティ事象の報告

[ISO/IEC27017 16.1.2]
お客様に大きな影響を与えるセキュリティインシデント（データの消失、長時間のシステム停止など）が発生した場合は、インシデントを検出してから 72 時間以内を目標に、以下のいずれかの手段にて、インシデントの内容や対応状況に関する通知を行います。

a. 当サービスの管理画面内に掲示
b. 当サービスのサポートページに記載
c. 当サービスのシステム管理担当者として登録されているアドレス宛にメールにて

お客様がセキュリティインシデントを発見した場合の報告およびセキュリティインシデントに関するお問合せにつきましては、カスタマーサポートにて受け付けております。進捗状況は個別にお客様にご連絡致しますが、調査の上でお客様に大きな影響を与えるセキュリティインシデントが発生していることが判明した場合は、前述の通り 72 時間以内を目標に通知致します。

3.8.4. 監査の受け入れ

障害発生時は早期復旧と対応を優先させるため、監査は受け入れておりません。ただし、障害の経緯に関する報告書を提出することは可能です。担当営業に個別にご相談ください。

3.8.5. 代替機能の提供

当サービスでは、ディザスタリカバリーサイトは準備しておりません。現在は遠隔地バックアップに留まりますが、今後の対応を検討しております。なお、可能な場合は遠隔地バックアップより、お客様へのデータの返却を検討致します。

3.8.6. 復旧時間

当サービスでは障害発生時の目標復旧時間を設けておりません。また、平均復旧時間は非開示とさせていただきます。

3.8.7. 過去の情報漏えい事故

過去において、個人情報の漏えい事故は発生しておりません。

3.9. サポート体制

3.9.1. サポート内容

操作方法や仕様に関するご質問、ご要望並びに不具合の報告を承ります。ただし、当サービス、あるいは当サービスのご利用に関係する事項と致します。

3.9.2. 問い合わせ方法

問い合わせは電子メール、電話、問い合わせフォームにて受け付けております。

3.9.3. 対応時間

土曜日、日曜日、国民の祝日、年末年始（12 月 28 日から 1 月 4 日）、および当社所定の休日を除く、平日 10:00～12:00 および 13:00～18:00 を回答時間とします。ただし、障害時は障害状況に応じて延長のご連絡を致します。また、カスタマーサポートへのお問い合わせには通常翌営業日までに回答を致します。

3.10. 月間稼動率

3.10.1. 目標値

当サービスの提供時間は、計画停止や定期メンテナンスを除いて 24 時間 365 日となります。
また、クライアント機能の月間稼働率は 99%以上、コンシューマ機能の月間稼働率も 99%以上となることを目標と致します。
詳細は「Synergy!サービス品質保証制度」の「第4章 報告制度について」にございます「第2節 報告項目（クライアント機能月間稼働率）」「1. 目標値」および「第3節 報告項目（コンシューマ機能月間稼働率）」「1. 目標値」をご確認ください。

3.10.2. SLA 報告制度

当サービスでは、より良いサービスの提供およびサービス品質に対する PDCA サイクルの構築を目的として、SLA の報告制度を設けております。数値化できる品質指標を報告項目と定め、月次にて目標値とその達成状況を報告させていただいております。詳細は「Synergy!サービス品質保証制度」の「第4章 報告制度について」をご確認ください。

3.11. 開発体制

3.11.1. 開発環境

当サービスは、本番環境と分離したステージング環境において十分検証した後に本番環境に適用しております。なお、ステージング環境はお客様には公開しておりません。

3.11.2. 本番データの利用

「Synergy!契約規定」の「第 10 条 情報管理」に基づき、当社は DB 格納情報を法令で認められた範囲または本サービスの保守業務に必要な範囲に限り、社内承認を得た上で利用致します。当社は上記に該当する場合を除き、DB 格納情報をお客様の承諾なく利用し、第三者へ提供することはございません。また、DB 格納情報に個人情報が含まれる場合は、個人情報の保護に関する法律を遵守します。

3.11.3. 開発におけるセキュリティ基準

[ISO/IEC27017 14. 2. 1]
開発に際しては、OWASP や IPA の安全なウェブサイトの作り方などを参照しております。また、開発に際しては品質保持のためリードエンジニアによるプログラムのソースコードのレビューを、製品リリースや稼働中のシステムの設

定変更を行う場合にも、レビュープロセスの実施を必須としております。

3.11.4. ソースコードの管理

当サービスのソースコードは、バージョン管理システムにより管理されております。利用しているバージョン管理システムの製品名は非開示とさせていただきます。バージョン管理システムへのアクセスは、承認により開発者に付与しております。

3.11.5. 本番環境へのリリース

本番環境へのリリースは、定められたプロセスを経て行います。なお、本番環境へのリリースは CI/CD システムを通して実施致します。採用している CI/CD システムの詳細は非開示とさせていただきます。CI/CD システムを操作する権限は、承認の上付与しております。

3.11.6. ぜい弱性管理

[ISO/IEC27017 12.6.1]
当社は自動診断ツールによるアプリケーションぜい弱性診断を週次で実施しているほか、自動診断ツールによるネットワークぜい弱性診断を日次で実施しております。また、JVN のぜい弱性情報を定期的に確認しております。なお、ペネトレーションテストは実施しておりません。

3.12. 保守体制

3.12.1. VDI

本番環境へのアクセスなど保守業務を実施する際は、VDI を経由する必要がございます。VDI は大阪本社のネットワークからのみアクセスが可能となります。社外からアクセスする場合は VPN にて大阪本社のネットワークにアクセスする必要がございます。VPN にログインするには、パスワードおよびソフトウェアトークンによる多要素認証が必要となります。VDI 環境からインターネットへのアクセスは制限しております。
なお、VDI のアカウントは、承認の上必要最小限の保守要員に付与しております。

3.12.2. データーセンターおよびサーバへのアクセス

当サービスのサーバなどのインフラストラクチャーには、VDI より AWS の管理ツールを用いてアクセス致します。VDI から AWS への通信はインターネットを経由します。通信は暗号化されております。AWS 管理ツールへのログインには、パスワードとワンタイムパスワードの多要素認証が必要となります。
サーバにアクセスするのためのパスワードにつきましては、「アクセス権限管理細則」にてパスワードポリシーを策定し

ております。パスワードは次の条件を満たす必要がございます。

- 第三者が容易に推測できない文字列を使用すること
- 8 文字以上の長さにすること
- 下記 4 つのグループから最低 3 グループを使用すること
  - 英字の大文字
  - 英字の小文字
  - 数字
  - 特殊記号

なお、パスワードの定期的な変更につきましては、総務省通達を鑑みて義務づけておりません。

3.12.3. データベースサーバーへのアクセス

データベースサーバへのログインにつきましては、ログイン発生時に複数の関係者に通知するよう設定しており、計画外のアクセスは検知されます。また、データベースの監査ログを取得し、1年間保存しております。

3.12.4. アクセス権の管理

保守作業に必要なシステム ID の発行につきましては、管理者による承認の上、必要なものにのみ発行しております。またシステム ID は個人単位で発行しており、共有しておりません。また、申請者と承認者は別の者となります。

3.12.5. 特権アクセス権の管理

システムを管理するための特権アカウントは、システム管理部門のみが利用できるようにしており、定期的に棚卸しを行っております。また、特権アカウントは利用者情報と紐づけることで、誰が利用したかを把握できるようにしております。

3.12.6. 退職者および異動者の対応

システム ID の棚卸しを定期的に実施し、異動や退職により不要になったシステム ID を破棄しております。

3.12.7. 容量・能力の監視

[ISO/IEC27017 12.1.3]
当社は当サービスにおける各種リソースについて、容量・能力を 24 時間 365 日監視しており、必要に応じてリソース増強を計画、実施しております。当社が監視している項目は次のような項目となります。

- サービスが正常に起動しているか
- 各種ネットワークサービスが正常に応答するか
- 負荷が想定している一定値以下か
- リソースの利用率が想定している一定値以下か

上記以外にも各機器の役割によって監視を設定しております。

3.12.8. ログの記録およびログの保護

[ISO/IEC27017 18.1.3]
当サービスを構成する各サーバにおける当社保守作業、および各サーバへのアクセスは全て自動的に記録されます。顧客データベースの監査ログも取得しております。
当サービスの保守を目的として記録したログは 1 年間保存しておりますが、定期的な分析は行っておりません。また、改ざんを防ぐために、通常のサーバ群とは異なる権限管理がなされた別サーバに集約して保存しております。

3.13. その他

3.13.1. 証拠の収集

[ISO/IEC27017 16.1.7]
法令に基づく場合および監督官庁または捜査機関による指導・摘発・注意もしくは照会を受けた場合は、情報を開示することがございます。

3.13.2. 適用法令

[ISO/IEC27017 18.1.1]
当社は日本の法人であり、日本国法が適用されます。当サービスのシステムは AWS を利用して構築しており、システムが保管するデータおよびそのバックアップデータは、いずれも AWS の管理するデータセンタ（東京リージョンおよび大阪リージョン）に保管されております。また、AWS との契約においては準拠法を日本国法とする契約を結んでおり、これにより海外法の適用によるリスクを回避しております。

また、当社はプライバシーマーク制度および情報セキュリティマネジメントシステム（ISMS）に適合している企業として認証を受けており、加えて、当サービスは ISMS クラウドセキュリティ認証に適合しているクラウドサービスとして認証を受けおります。当社および当サービスは、これらの外部認証が要求する法令等を遵守しております。

3.13.3. 知的財産権

[ISO/IEC27017 18.1.2]
以下の知的財産権は、お客様に帰属致します。

- 当サービスにお客様が格納された個人情報を初めとする顧客データ
- 当サービスでお客様が設定されたフォームや web ページの内容※
- 当サービスでお客様が配信されたメールやアプリプッシュの件名や内容※
- その他、当サービスでお客様が配信されたもの※

※ただし、当社に作成を委託された場合は、委託契約の内容に従います。

上記を除く知的財産権は、当社に帰属致します。これには以下のものが含まれます。

- 当サービスのソースコード
- 当サービスの管理画面、サポートページのデザインや内容
- 当サービスの設計、仕様
- 当サービスのアイデア、コンセプト、企画、創作

知的財産に関するお問い合わせは、カスタマーサポートにて承ります。

3.13.4. サービスの終了

当社は「Synergy!契約規定」の「第 16 条　当社による本サービスの終了」に基づき、お客様に6ケ月前までに通知を行った上で、当サービスの全部または一部の終了を行うことができるものとします。代替手段は提供致しませんが、クライアント機能の管理画面より、お客様にてデータのエクスポートは可能です。なお、通知方法は「Synergy!契約規定」の「第 4 条　通知」の通り、以下のいずれかと致します。

① お客様が予め指定した電子メールアドレス宛（管理者メールアドレス）に電子メールを送信して行う
② 当サービスのトップ画面にメッセージを掲示して行う

3.13.5. 反社会的勢力への対応

当サービスのご利用においては「Synergy!契約規定」の「第 32 条　反社条項」に基づき、反社会的勢力又は反社会的勢力と関与したことが判明した場合、何らの事前の通知および催告なしに、直ちに本契約を含む相手方とのすべての契約の全部または一部につき、何らの責任を負うことなく、その債務の履行を停止し、また停止することなく直ちに解除することができることと致します。

3.13.6. 損害賠償

損害賠償につきましては「Synergy!契約規定」の「第 31 条　損害賠償」に基づき対応致します。

3.13.7. 紛争解決

「Synergy!契約規定」の条項または「Synergy!契約規定」に定めのない事項について紛議等が生じた場合は、「第 34　条　紛争の解決」に基づき、できる限り円満に解決するものと致します。なお、本契約に関する紛争は大阪地方裁判所又は大阪簡易裁判所を第一審の専属的合意管轄裁判所と致します。

3.14. 補足

[ISO/IEC27017 15.1.2]
当社が実施するお客様に関係するセキュリティ対策は以下の通りです。当ドキュメント内に記載がある場合、項目番号および項目名のみ記載しております。

セキュリティ対策事項	対策内容
マルウェアからの保護	● 3.3.11 仮想マシンの要塞化
バックアップ	● 3.3.7 バックアップ
暗号による管理策	● 3.3.8 暗号化 ● 3.3.9 暗号化機能に対する規制
ぜい弱性管理	● 3.11.6 ぜい弱性管理
インシデント管理	● 3.8.3 情報セキュリティ事象の報告
技術的順守の確認	● 3.11.3 開発におけるセキュリティ基準
セキュリティ試験	● 3.11.6 ぜい弱性管理
監査	当社は、ISO/IEC27001 およびプライバシーマークについて第三者による審査を受け、それぞれの認証を取得しております。
ログ及び監査証跡を含む証拠の収集、保守及び保護	● 3.12.8 ログの記録およびログの保護 ● 3.13.1 証拠の収集
サービス合意の終了時の情報の保護	● 3.4.13 顧客データベースの削除
認証及びアクセス制御	● 3.4.2 クライアント機能へのアクセス
アイデンティティ管理及びアクセス管理	● 3.4.8 ユーザの登録および削除 ● 3.4.9 ユーザのアクセス権限設定 ● 3.4.10 ユーザの秘密認証情報の管理 ● 3.4.11 情報へのアクセス制限