

## 第2号様式（2）：非機能要件

非機能要件			事業者 チェック欄
大項目	中項目	要求水準	
セキュリティ	データセンターの設置場所	データセンターは、日本国法を準拠法とし、日本国内に所在する裁判所が当該紛争又は訴訟についての専属的裁判管轄権を行使できる環境であること。	
	SSAE16 SOC1 準拠 SSAE16 SOC1 Compliant	CRM サービスが SSAE16 SOC1 に準拠していること。	
	セキュリティ監査	CRM ベンダーのアプリケーションのセキュリティ監査を第三者機関によって実施した顧客に関する詳細情報を提供できること。	
	シングルサインオン	SAML トークンによるアクセス保護を提供していること	
	プロビジョニングとプロビジョニング解除	企業の LDAP ディレクトリからユーザを一元的に管理できるシステムが用意されていること。	
	2要素認証	パスワードと PIN を組み合わせた認証のオプションが用意されていること。	
	設備を保護する物理的なセキュリティ	サービスをホストする施設が、ビデオによる監視、火災や浸水の検知システム、生体認証、24時間体制の警備、フリーアクセスフロア（二重床）などの物理的なセキュリティ体制を備えていること。	
	侵入検知	内部ネットワークと外部ネットワークの各所に侵入検知システムを設置していること。	
	SSL によるセキュリティ SSL Security	256 ビット SSL による暗号化に対応し、HTTPS をサポートしていること。2048 ビット RSA 公開鍵に対応していること。	
	Web アプリケーションのセキュリティ	安全なセッション Cookie を利用でき、クライアントでユーザ ID とパスワードを入力する必要がないこと。クロスサイトスクリプティングや SQL インジェクションを防止できること。	
	必要に応じて厳格なパスワードポリシーを適用できること	パスワード長の下限、パスワードの再利用の制限、無効なパスワードが入力された場合のロックアウトなどを設定できること。	
	パスワードの保管	256ビットハッシュ SHA2 アルゴリズムにより顧客パスワードが保存されていること。	
	クラウド事業者の顧客データへのアクセス	メンテナンスやサポート用に顧客データにアクセスできるユーザー権限をクラウド事業者が有していないこと	
	ネットワークアクセス	IP制限機能を備えること	
	公的認証取得の要件	「ISMSクラウドセキュリティ認証」等のガイドラインで定められる資格を有していること	
	第三者評価	有（外部機関により脆弱性の評価を受け対策を講じる等）	
	通信の暗号化レベル	SSL、あるいはVPN。SSLの場合は、SSL3.0/TLS1.0以上に限定	
	ユーザーログ (アクセス・イベント)	ユーザーがどの IP アドレスからどのデータにアクセスし、そのデータに関連してどのようなアクションを取っているか認証可能であること	
	監査証跡	要求時に、上記ログの取得・開示または、潜在的な不正使用の有無を識別する報告を提供できること	
	セキュリティ監視	セキュリティ関連のイベントをモニターして、成功アクセスも不成功（拒否）アクセスも記録していること。また条件に応じて通知がなされること	
可用性	サービス時間	24時間365日（計画停止/定期保守除く）	
	サービス稼働時間	99.9%以上（基幹業務） 99%以上（基幹業務以外）	
	ディザスタリカバリ	遠隔地のバックアップ用データセンターで保管しているデータと予備システムへの切替	
信頼性	システム監視基準	1日4回以上のシステム/ネットワーク/パフォーマンス監視	
	障害通知プロセス	指定された連絡先にメールで通知または自サービスのページで状況の通知	
	平均復旧時間	1時間以内（基幹業務）、3時間以内（基幹業務以外）	
拡張性	カスタマイズ性	設定画面上の項目のカスタマイズまたは何らかのプログラミング言語により開発可能	
	外部接続性	外部公開されているAPIが提供されていること	
	同時接続利用者数	30ユーザー（ベストエフォート型）	
データ管理	データ保管	規定容量以内であればサービス契約期間内で有期であること	
	バックアップ保存基幹	・バックアップ取得期間：1ヶ月間分 ・ログ保管期間：13ヶ月以上、基幹データ：3年以上	
	ハウスキーピング	標準で、システム上不要データ等の定期削除実行の機能を保持すること	
サポート	システムサポート	提供サービスが主体であるテクニカルサポート窓口を保持すること	
	オンラインリソース	ベストプラクティス、ブログ、ユーザグループ、導入支援などのオンラインリソースをはじめとする無料のサービスを提供していること。	
	管理項目取得機能	システムの管理者がユーザ登録数などのデータを閲覧できること	

※「事業者チェック欄」については、要件を満たしている項目に○を記入すること。（要件を満たしていない項目があれば提案不可）