

INFORMATION SECURITY REPORT

情報セキュリティへの取り組み

スマート L クラウドを安心してご利用いただくために

OUR COMMITMENT

お客様からお預かりする情報を適切に保護し、安心してサービスをご利用いただける環境を継続的に整備します。

私たちが重視する 3 つの観点

情報の保護 INFORMATION	安定したサービス提供 CONTINUITY	継続的な改善 IMPROVEMENT
----------------------	--------------------------	-----------------------

情報セキュリティに対する考え方

信頼されるサービス提供の基盤として、情報セキュリティを継続的に改善します。

株式会社リクモは、お客様が安心してサービスを利用できるよう、情報の保護と安定したサービス提供を重要な経営課題の一つと捉えています。

本資料では、当社の情報セキュリティに関する基本的な考え方と、スマートLクラウドにおける主な取り組みをご紹介します。公開資料として、具体的なシステム構成、設定値、監視条件等の詳細は記載していません。

本資料の目的

取引先・お客様に、当社の情報セキュリティに対する姿勢、主要な管理策、障害・セキュリティインシデント発生時の基本的な対応方針をご理解いただくことを目的としています。

対象範囲

会社の取り組み	株式会社リクモの情報管理および情報セキュリティに関する取り組み。
サービス	スマートLクラウド。個別開発システムや外部サービスの仕様は対象外です。
詳細情報	取引上必要な場合は、契約・セキュリティ審査等に応じて個別にご案内します。

CONTENTS

02	認証・セキュリティ宣言・専門資格	06	障害の影響度判定
03	業務における情報の取り扱い	07	影響度に応じた対応目標
04	スマートLクラウドの主な情報セキュリティ対策	08	お問い合わせ・関連情報
05	障害・セキュリティインシデントへの対応		

認証・セキュリティ宣言・専門資格

第三者の枠組みや専門資格を活用し、情報セキュリティとサービス品質の向上に取り組みます。

ISMS

ISO/IEC 27001 認証取得

情報セキュリティマネジメントシステムの国際規格である ISO/IEC 27001 の認証を取得しています。

認証番号：816589/C/1

IPA

SECURITY ACTION 「一つ星」

情報処理推進機構（IPA）が推進する SECURITY ACTION の「一つ星」を自己宣言しています。

LINE

LINE Green Badge 取得者が在籍

LINE サービスに関する知識・運用スキルを認定する LINE Green Badge の取得者が在籍しています。

位置づけについて

各認証・宣言・資格は、それぞれ対象や制度上の位置づけが異なります。LINE Green Badge は個人を対象とする資格であり、株式会社リクモまたはスマート L クラウド自体のセキュリティ認証を示すものではありません。

業務における情報の取り扱い

情報のライフサイクル全体を意識し、必要な管理・監督・見直しを行います。

必要な範囲での情報利用 取得した情報は、公表した利用目的およびサービス提供に必要な範囲で取り扱います。	安全管理措置 情報の漏えい、滅失、毀損等を防止するため、必要な安全管理措置を講じます。
従業者・委託先の管理 情報を取り扱う従業者や委託先に対して、必要な管理・監督を行います。	アクセス範囲の管理 業務上必要な範囲に応じて、情報へのアクセスを制御します。
外部サービスとの区分 第三者が提供する外部サービスについては、当社サービスと責任範囲を区別して取り扱います。	継続的な見直し 情報セキュリティを取り巻く環境やサービスの変更に応じ、取り組みを継続的に見直します。

プライバシーポリシーとの関係

個人情報の取得・利用目的、第三者提供、開示・訂正等の手続きについては、当社のプライバシーポリシーをご参照ください。

スマート L クラウドの情報セキュリティ対策

複数の対策を組み合わせ、情報の機密性・完全性・可用性を意識した運用を行います。

認証・アクセス制御 利用者の認証と、役割・担当範囲に応じたアクセス制御を行い、必要な範囲に情報アクセスを限定します。	通信・保存情報の保護 通信中および保存される情報に対し、暗号化等の必要な保護措置を講じます。
不正アクセス対策 Web アプリケーションへの不正なアクセスや攻撃に対し、検知・制御するための仕組みを導入しています。	監視・ログ管理 サービスの状態を監視し、運用上必要なログを取得・管理することで、異常の早期把握と調査に備えます。
バックアップ サービス継続や障害からの復旧に備え、必要なバックアップを取得・管理します。	変更・運用管理 システムの変更・リリースについて管理し、安定したサービス提供に努めます。

公開範囲について

具体的なシステム構成、製品・サービス名、設定値、検知条件、保持期間等は、セキュリティ上の理由から本資料では公開していません。取引上必要な場合は、必要性和開示範囲を確認のうえ個別に回答します。

障害・セキュリティインシデントへの対応

発生時の初動から復旧後の改善まで、一連の対応を継続的な品質向上につなげます。

障害やセキュリティインシデントを把握した場合は、影響を確認し、必要な初動・復旧・お客様へのご案内を行います。対応後は原因や対応内容を振り返り、再発防止と継続的な改善につなげます。

01 検知・受付 監視やお問い合わせ等から、障害・異常を把握	02 影響確認 ユーザー範囲・機能範囲等を確認	03 初動・拡大防止 必要な初動対応を実施
04 お客様へのご案内 確認できた内容と対応状況を案内	05 復旧・確認 復旧対応と正常性確認	06 原因確認・改善 原因整理と再発防止・改善

関係者の連携

事象の内容と影響に応じて、開発・運用・顧客対応等の関係者が連携し、影響の把握、復旧、お客様へのご案内を進めます。

情報開示の考え方

内部の監視条件、技術的な検知閾値、エスカレーション経路等の詳細は公開していません。

障害の影響度判定

ユーザー範囲・機能範囲・回避可否を組み合わせ、対応の優先度を4段階で判定します。

障害発生時は、「影響を受けるユーザーの範囲」「影響を受ける機能の範囲」「代替手段による回避の可否」等を確認し、影響度を Critical / High / Medium / Low の4段階で判定します。

機能範囲	利用状況	回避可否	全ユーザー	一部ユーザー
全機能	全機能に影響	回避不可	Critical	High
全機能	全機能に影響	回避可能	Medium	Low
一部機能	通常業務利用	回避不可	High	Medium
一部機能	通常業務利用	回避可能	Medium	Low
一部機能	普段使わない	回避不可	Medium	Low
一部機能	普段使わない	回避可能	Low	Low

※「全ユーザー」は影響を受けるユーザー範囲が全ユーザーである場合、「全機能」は影響を受ける機能範囲が全機能である場合を指します。

※影響度は障害対応の優先度を判断するための基準です。

影響度に応じた対応目標

判定した影響度に応じて、初動・復旧の優先順位を設定します。

影響度の高い事象ほど優先的に対応し、サービス影響の早期解消に努めます。応答時間は事象を認識してから初動対応を開始するまでの目安、復旧目標はサービスまたは対象機能を利用可能な状態へ戻すことを目指す時間の目安です。

影響度	応答時間	復旧目標	定義（概要）
Critical	15 分（目標）	4 時間（目標）	サービス全体停止、または中核機能が全ユーザーで利用不可。回避策なし。
High	1 時間	1 営業日（目標）	主要機能が著しく劣化。多数ユーザーに影響。回避策が困難。
Medium	1 営業日	5 営業日（目標）	一部・周辺機能の不具合。回避策あり。
Low	2 営業日	次回リリース	軽微な不具合・表示崩れ・質問等。

対応後の改善

重大な障害やセキュリティインシデントについては、原因と対応内容を整理し、必要な再発防止策や運用改善につなげます。

目標値の取り扱い

上記対応時間につきましては、営業時間内に発覚したものを基本としております。発生時刻に応じて、対応完了時間が伸びる可能性がございますことをご了承ください。

※応答時間・復旧目標は目安であり、事象の内容、影響範囲、原因、外部サービスの状況その他の事情により変動する場合があります。個別契約に別段の定めがある場合は、その内容が優先されます。

お問い合わせ・関連情報

セキュリティ確認や個別の審査については、必要性和開示範囲を確認のうえ対応します。

セキュリティに関するお問い合わせ

サービス導入時のセキュリティ確認や、本資料の内容に関するご質問は、当社担当者または下記窓口へお問い合わせください。

株式会社リクモ

info@likumo.com

関連情報

- [株式会社リクモ 公式サイト](#)
- [株式会社リクモ プライバシーポリシー](#)
- [ISO/IEC 27001 \(ISMS\)](#)
- [IPA「SECURITY ACTION」](#)
- [LINE Green Badge](#)

個別のセキュリティ確認について

取引先様のセキュリティチェックシートや個別の確認事項については、必要性および開示範囲を確認のうえ、個別に対応します。

株式会社リクモ / 情報セキュリティへの取り組み 2026 / 第4版