



Security White Paper

ラクスル株式会社
セキュリティホワイトペーパー
2024年5月10日発行



はじめに - 本ホワイトペーパーについて

この文書は、2024年2月時点におけるラクスル株式会社（以下「当社」といいます。）の情報セキュリティへの取り組みと、情報セキュリティの観点からお客さまにご注意いただきたい点について紹介するものです。当社は、パンフレットやノベルティグッズへの印刷、ポスティングやダイレクトメール等の配布、梱包資材等の販売を行うサービスとして、「ラクスル」「ダンボールワン」「ラクスルエンタープライズ」を提供しております。お客様よりデザインや宛名のデータをお預かりし、印刷・製本や封入などを経てお客様またはお客様のご指定の宛先へ納品するサービスとなります。

当社ではお客様からお預かりするデザインデータや宛名データを重要情報として扱います。お客様の意思に反して第三者に読み取られたり、内容を改ざんされることがないように、情報セキュリティに配慮した慎重な取り扱いを行います。

本ホワイトペーパーでは、当社の提供する各サービスをこれからご利用いただく予定の方だけでなく、今お使いの方に対しても、サービスのご利用に際しデータセキュリティとプライバシー保護についてどのように対処しているかご説明致しますので、ぜひご活用ください。

本ホワイトペーパーでご説明する内容

本ホワイトペーパーでご説明する情報セキュリティの取り組みの範囲は、当社で運営する以下のサービスに関するものです。

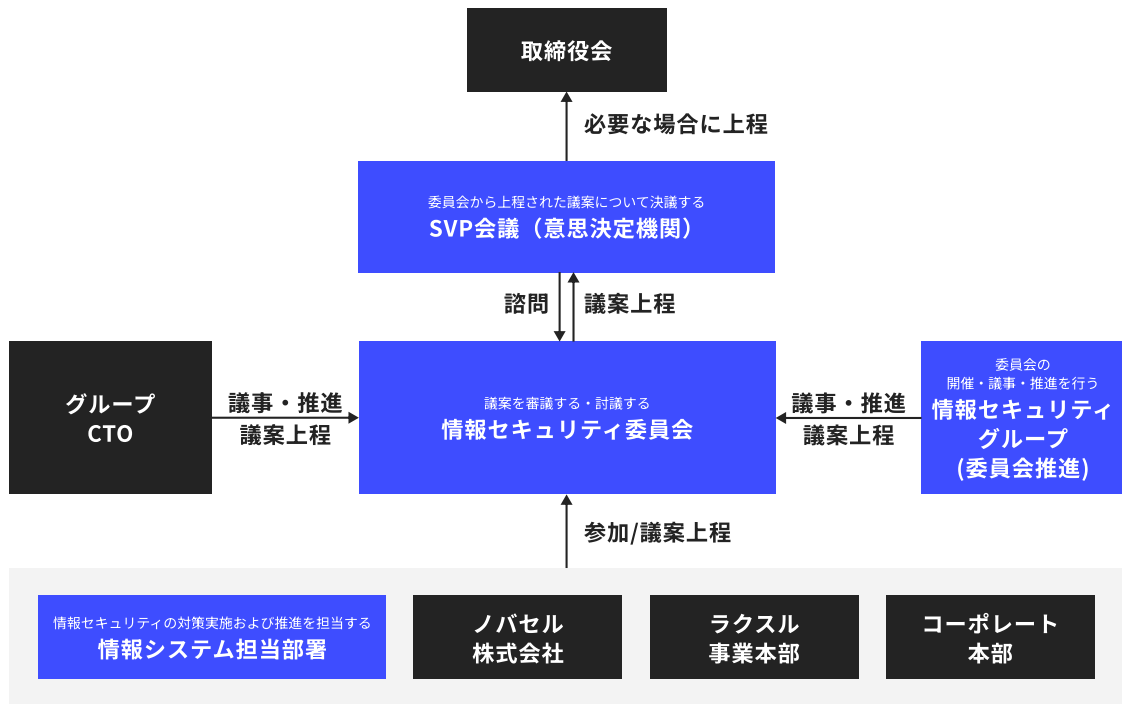
- ラクスル
- ダンボールワン
- ラクスルエンタープライズ

当社では情報セキュリティ方針や個人情報保護方針、プライバシーポリシーについて以下の文書を公開しております。

- 情報セキュリティ基本方針
<https://corp.raksul.com/security-policy/>
- 個人情報保護方針及びラクスルグループにおける共同利用について
<https://corp.raksul.com/privacy-policy/>
- ラクスル株式会社における個人情報の取り扱いについて
<https://corp.raksul.com/privacy/>
- ラクスル
 - ラクスルサービスにおける個人情報の取り扱いについて
<https://raksul.com/privacy/>
- ダンボールワン
 - ダンボールワンサービスにおける個人情報の取り扱いについて
<https://www.notosiki.co.jp/contents/company/privacy.html>

情報セキュリティとプライバシー保護の体制について

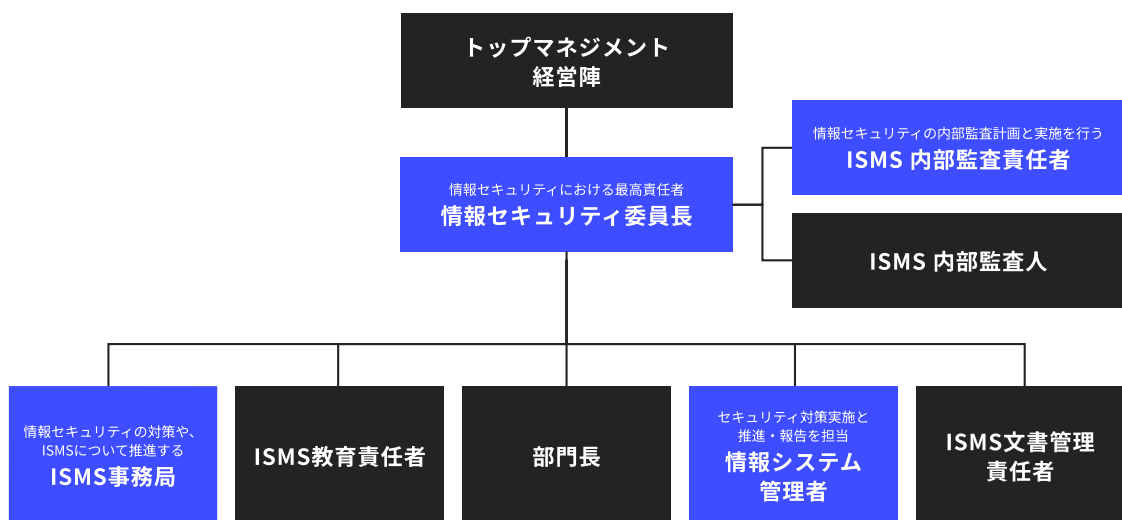
当社では、グループ全体の情報セキュリティ方針の策定を担う情報セキュリティ委員会を組織し、情報セキュリティ委員会で議論された方針や計画にかかる具体的な施策の意思決定は、意思決定機関であるSVP会議にて行っています。



■ 委員会を中心となって活動する組織・セクション

情報セキュリティの体制

情報セキュリティ委員会の組織体制として下図の通り構成され、経営陣が情報セキュリティ委員長・内部監査責任者・事務局・教育責任者・文書管理責任者を任命し、情報セキュリティ体制を構築しています。



■ 委員会を中心となって活動する組織・セクション

第三者認証について

プライバシーマーク

個人情報保護法およびJIS Q 15001の要求に基づき対策を講じており、一般財団法人 日本情報経済社会推進協会（JIPDEC）より2年毎に外部審査を受け、プライバシーマークの認定を受けております。

認証番号	10824430 (04)
指定審査機関	一般財団法人日本情報経済社会推進協会(JIPDEC)
有効期限	2024年11月1日



情報セキュリティマネジメントシステム（ISMS）

情報セキュリティマネジメントの国際規格であるISO/IEC27001に基づく規定・基準を定めています。情報資産の損失、改ざん、サービス停止など、情報セキュリティを管理するシステム（ISMS）を構築、運用し、継続的に改善することにより、情報資産の機密性、完全性、可用性の維持に努めています。

ISMSに適合している企業として第三者認証機関であるBSI社から認証を受けており、当社の情報セキュリティ管理システムは国際基準に準拠していることが認められております。

認証登録番号	IS 665934
認証機関	BSIグループジャパン株式会社(ISR004)
認証基準	ISO/IEC 27001:2013(JIS Q 27001:2014)
有効期限	2025年10月31日



監査の実施

当社ではセキュリティ運用の監査・プライバシー保護についての内部監査を年1度以上実施しており、内部監査の結果は内部監査報告書を作成し、経営層へ報告しております。また、ISO/IEC27001の運用上、第三者認証機関による審査を毎年受けております。

お客様情報の取扱い

当社ではお客様の情報がビジネスの源泉であると考え、重要情報として位置づけております。

取得したお客様情報の利用

当社が取得したお客様情報の利用に当たりましては、利用目的を公表し、利用目的の範囲内でのみ利用します。詳しくは、「[ラクスルサービスにおける個人情報の取り扱いについて](#)」「[ダンボールワンサービスにおける個人情報の取り扱いについて](#)」のページをご参照ください。

ラクスルグループにおける共同利用

当社グループ会社におきまして、お預かりした個人情報を共同で利用致します。共同利用について、目的や項目についての詳細は「[個人情報保護方針及びラクスルグループにおける共同利用について](#)」のページ内「ラクスルグループにおける個人情報の共同利用について」にて記載しておりますので、ご参照ください。

RAKSUL VIETNAM LIMITEDへの提供

当社グループ会社のうち、RAKSUL VIETNAM LIMITEDは、ベトナム社会主義共和国に所在し、当社が提供するサービスの機能開発・保守・運用を委託している企業になります。当社とRAKSUL VIETNAM LIMITEDとの間では、当社で実施しているセキュリティ対策を同等の基準で実施する委託契約を締結し、セキュリティの確保をしております。

お客様情報の委託と委託先の管理

印刷パートナーやDMパートナー、運送会社など、多数の委託先へお願いすることによって当社のサービスは成り立っております。そのため、サービス提供において必要と考えられるパートナーに対して、お客様の情報を提供しております。委託先の選定に当たりましては、委託する業務や取扱う情報資産に応じてセキュリティ審査を行っており、基準に満たない場合の是正等を行っております。

提供される情報の内容について詳しくは、「[ラクスルサービスにおける個人情報の取り扱いについて](#)」「[ダンボールワンサービスにおける個人情報の取り扱いについて](#)」の「個人情報の利用目的」の項、および「[ラクスル株式会社 個人情報保護方針](#)」をご覧ください。

アクセス権限管理

お客様のデータに関しましては、それぞれのシステムでアクセス権限が設定されております。従業員ごとに付与される個別のIDを発行し、アクセス権限の管理をすることにより、許可の無い従業員がお客様のデータにアクセスができないように予防措置を講じております。

データの開示・訂正・削除

当社サービスにアカウントのご登録が存続する場合、お客様が当社サービスに対して登録した個人情報は、各サービスのマイページより訂正・削除することができます。

解約時のデータの扱い

アカウント解約時の個人データにつきましては、「[ラクスルサービスにおける個人情報の取り扱いについて](#)」「[ダンボールワンサービスにおける個人情報の取り扱いについて](#)」に基づき、当社所定の手続きでご請求いただいた場合、法律に従った範囲で削除を行っております。

研修の実施

当社ではお客様の情報を取り扱うスタッフのみならず、全ての従業員及び業務委託で当社システムにアクセスするパートナーの従業員に対して、セキュリティ・プライバシーの研修を実施しております。実施の結果については、コーポレートサイトのサステナビリティ・ESG経営(https://corp.raksul.com/esg/esg_data/#social)の中にあるESGデータ「従業員の研修」をご覧ください。

事故の報告

情報セキュリティ上の重大な事故（データの消失・毀損、情報漏洩、長時間のサービス停止など）、またサービス提供に関する重大な事故については、発生を検知し次第速やかにお客様へご連絡するため、以下のいずれかの方法で通知または公表等を行います。

1. 当社サービスへ登録されているメールアドレス宛にメールでのご通知
2. （エンタープライズ事業のみ）当社営業担当より個別に電話またはメールにてご連絡
3. 当社サービス上のトップページやお知らせへの掲示
4. 当社サービスのサポートページ等の記載

技術的対策

インフラストラクチャとデータセンター

当社の各サービスは、Amazon Web Service, Inc.（以下、AWS社）、Google, Inc（以下、Google社）のGoogle Cloud、Microsoft社Azureのクラウドコンピューティングプラットフォーム上に構築されており、お客様からのお預かりするデータはそれぞれのクラウド上に構築されたシステム（サーバ・ストレージ）上に保存されます。AWS社、Google社、Microsoft社は世界の主要各国にデータセンターを配置しており、その中で当社は主に東京（日本）リージョンを利用してサービスの提供を行っております。

当社サービスは各社のプラットフォーム上にホスティングされたインフラストラクチャで稼働しており、様々なサービスを組み合わせ利用し、構成されています。

暗号化

通信の暗号化

当社サービスではTLS1.2以上による暗号化プロトコルを用いて、お客様のブラウザからサービスサイトまでの通信の暗号化を行っております。

データの暗号化

お客様情報が記録されるデータベース・ストレージは暗号化が行われ、データの保護が行われます。

パスワードの暗号化

お客様の設定されるパスワードに関しては、ハッシュ関数により処理がなされた後の、復号ができない状態のハッシュ値のみが保管・管理されます。

バックアップ

当社ではサービス運営のためデータベースバックアップは日次で7世代取得しております。

タイムスタンプと時刻の同期

障害対応などの有事調査について、サービスの運営に必要なサーバ・ネットワーク機器類の時刻につきましては、NTPを用いて全台時刻の同期を行っており、一環的なログが取得できるように構成しております。

サイバー攻撃対策

サーバの要塞化・安定化

当社の提供する各サービスでは以下の構成を取り、要塞化を行っております。

- 配信サービスとしてCDNを用い、Webサーバとデータベースサーバに関してはインターネットから直接アクセスはできないプライベートセグメントに配置しています。
- セキュリティパッチの適用が必要な脆弱性が発生した場合、可否検討の上、可及的速やかにパッチを適用しております。
- 必要最低限のポートのみ開放を行っております。
- 各サービスは複数のサーバにより冗長化されており、安定したサービス提供が行われるように構成しております。

マルウェア対策

従業員の利用する各PCにはウイルス対策ソフトウェアとEDRがインストールされており、ファイルの検査と挙動について監視されており、不審な振る舞いやファイルを検知すると、隔離・検疫などの処理を致します。

DDOS対策/WAF

当社サービスではAWS WAF/AWS Shieldを利用しており、Webアプリケーションの脆弱性を利用した攻撃や、大量のパケット送信によるサービス妨害に対する予防措置を講じております。

開発・運用

サービス開発にあたっては、アジャイル開発に則っており、そのフレームワークとしてスクラムを採用して、効率的な開発を進めています。また、開発プロセスはDevOpsをベースとして、要件・設計・開発・検証・リリース・監視という流れでプロダクトの機能追加や改修を行っております。



開発環境の分離

エンジニアが作業を行う開発環境は本番環境からは分離されており、本番環境への影響がないように構成されています。また、本番環境の顧客データを用いた開発は行っておりません。

運用について

リリース後の運用と監視については、24時間365日のシステムによる自動監視がなされ、障害など異常が発生した場合はアラートが発報され、エンジニアがその対処に当たります。

お客さまにご注意いただきたい点

サービスの利用に必要な環境とソフトウェア

ラクスルのサービスはGoogle Chrome、Microsoft Edge、Firefox、Apple Safariなどの主要ウェブブラウザで動作します。最新版のウェブブラウザをご利用ください。

詳しくは、「[推奨環境について\(https://raksul.com/guide/environment/\)](https://raksul.com/guide/environment/)」をご覧ください。

お客さまの環境におけるセキュリティ上の注意点

アカウント登録時のパスワードにつきましてはお客様ごと固有のものですから、第三者に知られない様に管理をお願い致します。他社ウェブサービスなどのアカウントパスワードと同一にする使い回しは避けるようお願い致します。

お問い合わせ先

サービスの内容、セキュリティについてご不明な点がございましたら各サービスのカスタマーサポート窓口へご連絡ください。

- [ラクスル](https://raksul.com/contact/)
- [ダンボールワン](https://www.notosiki.co.jp/contents/inquiry/)
- [ラクスルエンタープライズ](https://enterprise.raksul.com/contact)

以上