楽! ラクス ライトクラウド

blastmail セキュリティガイドブック

株式会社ラクスライトクラウドが行っているセキュリティ対策のご説明及び
お客様のご利用におけるセキュリティ上の注意点

株式会社ラクスライトクラウド　https://blastmail.jp/

目次

はじめに

この度は、弊社サービスの「ブラストメール」のご導入・ご検討いただき、誠にありがとうございます。

「ブラストメール」は、弊社が運用管理するサーバーにブラストメールのソフトウェアをインストールし、インターネットを介してお客様にソフトウェアをご利用いただくサービスです。

導入が簡単で、インターネットに繋がる環境さえあれば、いつでもどこでもご利用いただくことができる非常に利便性の高いサービスとなっております。

弊社では、「ブラストメール」をお客様に安心してご利用いただくために、さまざまなセキュリティ対策を施しております。

本書では、本書改定日時点でのセキュリティ対策内容についてご説明しております。
予め、ご了承ください。

ブラストメールにおけるセキュリティ対策

管理画面におけるセキュリティ

ログイン ID とパスワードによるユーザー認証

アカウント毎にそれぞれ異なるユーザーID とパスワードが付与され、ログインをする時には、ユーザーID 及びパスワードの両方が求められるようになっています。

パスワード変更、パスワードロック機能

ユーザーは任意のタイミングでユーザー認証に利用するパスワードの設定ができます。
また、ユーザーが一定回数、パスワードを間違えてユーザー認証を行おうとした場合、自動的にログインロックがかかるようになっております。

管理画面との通信の暗号化

SSL(Secure Socket Layer) を使った暗号化通信によって行うことができます。
これにより、やりとりする情報が暗号化されるため、安心してご利用いただくことができます。

一定時間、無操作状態が続いた場合の強制ログアウト

ユーザーがログインし、操作せずに一定時間経過した場合、自動的にシステムからログアウトされるようになっています。これより、万一ログインしたまま席から長時間離れた場合でも第三者が不正に利用する危険性を減少させることができます。

メール配信におけるセキュリティ

SPF (Sender Policy Framework)

電子メールの送信元ドメインが詐称されていないかをしてもらうための仕組みです。
ブラストメールは SPF に対応していますので、設定を行うことにより、送信したメールが迷惑メールと誤判定されることを防ぎやすくなります。

DKIM (DomainKeys Identified Mail)

迷惑メール対策となる送信ドメイン認証技術です。
ブラストメールの 10,000 プラン以上のプランでは、標準機能としてご利用いただけます。

STARTTLS

STARTTLS とは、メール送信中のデータ通信を暗号化することで、外部からのハッキングや悪質なメール盗聴などを防ぐ技術です。
ブラストメールでは、Gmail アドレスへのメール配信時に標準利用されております。
そのため、一般的にセキュリティが厳しいと言われている Gmail のメールサーバーへも心配なく配信いただけます。

サーバー運用・管理上におけるセキュリティ対策

世界トップレベルのデータセンターを利用

世界トップレベルのクラウド基盤である、Amazon Web Service を利用し、高い稼働率の実現しております。
また、日本国内の複数の拠点に分散してサーバーを配備することで、データの保全性を高め、万がーの場合にも、迅速な対応が可能です。

定期的なバックアップの取得

定期的にデーターベースのバックアップを取得しており、万がー、システム運用障害に取得時点までのデータ復旧が可能です。

不要な通信の遮断

ファイヤーウォールを利用し、利用に必要な通信(HTTP/HTTPS/SMTP)以外は遮断し、弊社運用に必要な通信は、接続元の制御を厳重に管理しております。

ソフトウェアの脆弱性対策

サーバーにインストールされている各種ソフトウェアにおける脆弱性を発見・察知し、弊社がソフトウェアのアップデートが必要であると判断した場合には、動作検証を行った上でアップデートを実施する方針になっております。

サービス監視

サービスが起動しているかどうかの監視を常時行っており、万がー、異常が発生した場合には、警告メールがシステム管理者、運用者に届くようになっております。

外部機関による定期的なセキュリティ診断の受診

定期的に、外部の機関からセキュリティ診断を受け、脆弱性顕在化の防止に努めております。

弊社におけるセキュリティ対策

プライバシーマークの取得

2006 年 10 月にプライバシーマークを取得。個人情報保護マネジメントシステムによる、適切な運用を継続しています。
JIS Q 15001 に基づいて、個人情報の適切な運用を継続しています。

運用人員の制限

メンテナンス作業、サポート業務などは、限られた担当者があるアクセス用端末を経由してのみ作業できるようになっており、弊社内からしかアクセスできない構成になっております。作業時に必要となるアクセス用端末のログイン ID、パスワードは、厳重に管理しております。

物理的なセキュリティ

従業員のオフィスエリアへの入退出を管理し、外部の人間が立ち入る場合のルールを作成・運用管理しております。

業務利用パソコンに対する対策

従業員が利用するパソコンには、パスワード設定を義務付け、必ずウィルス対策ソフトをインストールしております。
また、そのウィルス対策ソフトは、確実に更新し、最新版に維持しております。

ブラストメールをご利用いただくにあたってのお願い

ブラストメールを安全に正しくご利用いただくために、下記事項をご確認ください。

- ユーザーID、およびパスワードは厳重に管理し、漏えいなどにはくれぐれもご注意ください。
  また、パスワードは定期的に変更することをお勧めいたします。

- 万が一の場合に備え、必要な情報はバックアップを保持してください。

- 必ず、受信者の同意に基づき、メール配信をお願いいたします。

- 届かないメールアドレス、もしくは、届かなくなったメールアドレスは、配信対象から除外するようにお願いいたします。
  それらのメールアドレスへ配信を続けると、スパムメールとして判定されやすくなり、配信したメールが届かなくなる場合がございます。