# セキュリティとコンプライアンスに関する
# ホワイト ペーパー


株式会社サテライトオフィス

**2025年 02月 19日（第4版）**

■ 情報セキュリティに関する基本方針

サテライトオフィスでは情報セキュリティに関して極めて重要な事項として取り扱います。定期的なセキュリティ教育および利用環境へのセキュリティに関する施策を実施し、また業務上のリソース（資料やメール等）をクラウドサービスに保管していることの認識、利用クラウドサービスの可用性、冗長性、バックアップポリシー等を理解した上で利用しております。

■ 独立した第三者による認定

ISO 27001：JIS Q 27001:2023（ISO/IEC 27001:2022）
ISO 27001 [JIS Q 27001:2023（ISO/IEC 27001:2022）] は最も広く認識されて受け入れられている独立したセキュリティ規格の 1 つです。サテライトオフィスプロダクト事業部ではISO 27001を取得しています。

ISO 27017：JIS Q 27017:2016（ISO/IEC 27017:2015）
ISO 27017 [JIS Q 27017:2016（ISO/IEC 27017:2015）] は、クラウド サービスに特化した、ISO/IEC 27002 に基づく情報セキュリティ制御の実践に関する国際標準です。サテライトオフィスプロダクト事業部ではお客様に提供するGoogle Cloud Platform、Microsoft Azure、Amazon Web Services上で稼働する全サービスの開発、提供、運用に関してISO 27017を取得しています。

プライバシーマーク
当社は、一般財団法人日本情報経済社会推進協会（JIPDEC）よりプライバシーマークの付与認定を受けております。「プライバシーマーク」とは日本工業規格JISQ15001「個人情報保護に関するコンプライアンス・プログラムの要求事項」に適合し個人情報について適切な保護体制を整備している事業者に付与される制度です。今後ともお客さまの重要な個人情報を取り扱う事業者として、個人情報保護方針のもとに個人情報保護の管理・運営を徹底していく所存です。

■クラウドサービス選定に関する方針

利用するクラウドサービスの選定にあたっては、クラウドサービスの提供元がISO/IEC 27001および27017を取得していることを必要要件とします。加えて具体的なアクセス制御としてID、パスワードによる認証と二要素認証の機能を備えていることを要件とします。

また、クラウドサービスに保管する全てのデータに対する知的所有権がクラウドサービスカスタマに帰属することを利用規約で明記していることも要件とします。

さらに、クラウドサービスの運営法人および地理的所在、準拠法および関連当局情報について、また、サービスプロバイダとカスタマそれぞれの役割や責任の範囲についてや、監査ログの収集や開示、データ暗号、資産の処分や再利用ポリシー、知的財産権等に関する方針を把握した上でクラウドサービスを利用しております。

また、クラウドサービスは常に機能の追加や廃止、動作変更が行われる可能性があることを理解した上で適切な利用、運用を行っております。
■インシデント管理および障害時の連絡体制

サテライトオフィスでは、サテライトオフィスがお客様に提供するサービスに関して障害が発生した場合、インシデントとして管理し、重大度に応じて優先順位を設定し対処します。
お客様に直接影響が及ぶ事象については最優先で処理されます。
インシデントの内容によっては、サービス稼働プラットフォームのサポート窓口とも連携して事象の原因特定、解決に努めます。
またインシデントの内容に応じて弊社が必要と判断した場合は、自社の障害窓口サイトへの掲載およびメールでのお客様への通知を行います。掲載、通知までの目標時間は事象発生から1時間以内とします。また、インシデント内容の公開範囲は都度判断して決定するものとします。

■知的財産権についてのお問い合わせ窓口

サテライトオフィスが提供するサービス上に作成するコンテンツ、データの所有権、管理責任はお客様に帰属いたします。知的財産権に関してご不明点がありましたら、弊社サポート窓口（https://shurl.jp/171ZH）までお問い合わせください。

■サービスの機能追加や仕様変更のご案内

サテライトオフィスの各サービスは日々機能拡張、改善対応を行っております。それらの対応は基本的には既存機能に対する互換性を保った形で行われますが、もしお客様の既存運用への影響や管理者様の作業を伴う対応を行う場合は、十分な猶予期間を持った形で、メルマガ及びホームページへの記載などでお客様にご連絡いたします。
なおそれ以外の機能拡張についても同様の方法でご案内することがございます。

■ 全社員対象のセキュリティ教育

サテライトオフィスでは全社員を対象に、最新のセキュリティの脅威や脆弱性情報を下にした定期的なセキュリティ教育を行っています。

■ 脆弱性の管理

サテライトオフィスは、定期的に自動または手動による侵入テスト、ソフトウェアのセキュリティ検査を行っています。脆弱性が発見された場合は、社内のインシデント扱いとし、速やかに対応を行います。なお、通常、これらのテストの実施状況、結果については公開しておりません。

■ セキュリティを考慮した開発体制

サテライトオフィスではセキュリティおよび品質の維持を考慮した開発手順を定義し、定義に沿って開発、テスト、デプロイ、運用プロセスを実施しています。

■サービスの可用性、監視体制について

サテライトオフィスの各サービスは負荷状況に応じて自動的に冗長化する仕組みで動いており、急激な負荷に対しても全く問題なく安定稼働し続ける仕組みでご提供しております。また、各リ

ソースの監視も24時間365日行っており、万が一の障害にも迅速に対応できる体制を整えております。

■マルチテナントデータの分離について

マルチテナント形式でお客様にご提供しているクラウドサービスについては、論理的あるいは物理的にテナント間のデータ領域を分離したセキュアな環境でサービスを運用することとします。

■サービス稼働プラットフォームのクロック同期について

サテライトオフィスの各サービスはGoogle Cloud Platform、Microsoft Azure、Amazon Web Servicesといったプラットフォーム上で稼働しており、各プラットフォームのクロック同期は、Google Public NTP や time.windows.com 等の非常に実績のあるNTPサーバーで行っております。