

Contentsquareセキュリティ基準

[バージョン 2025.1.(2025年6月)]

1. Contentsquareは、顧客と調整し、必要に応じて、顧客データの処理、保存及び保護に関して顧客が書面で合理的に要求したすべての情報を顧客に提供するために、完全な資格のあるセキュリティチーム (security@contentsquare.com) を指定する。
2. Contentsquareは、適切な組織的、管理的、技術的及び物理的な保護措置並びに業界標準であり、Contentsquareが処理する顧客データの性質に見合ったその他のセキュリティ対策を含む、顧客データを保護するための書面によるデータ情報セキュリティプログラム(以下「情報セキュリティプログラム」という。)を実装し、維持している。Contentsquareの情報セキュリティプログラムには、顧客データのセキュリティに対するリスクの定期的なリスク評価を含む、これらのポリシー、採用及び退職手順に関する従業員の定期的なトレーニングが含まれており、適用される法律の変更による必要に応じて更新されるものとする。Contentsquareは、かかる更新又は変更が顧客データのセキュリティの重大な低下をもたらさないことを条件として、かかる措置を随時更新又は変更する権利を留保し、それを行うことができる。
3. Contentsquareは、顧客データの処理によってもたらされるリスク、特にContentsquareが保存又は処理する顧客データへの違法かつ不正な破壊、紛失、開示、又はアクセス(以下「セキュリティ侵害」という。)によるリスクに適切なレベルのセキュリティを確保するために、適切な物理的、技術的、及び組織的対策を実施するものとする。かかる対策には、とりわけ、以下の対策が含まれる。
 - (i) 人為的又は環境的な原因による顧客データへの不正な物理的アクセス又は侵害を防止するための、クラウドサービスを通じた合理的かつ十分な物理的障壁及び制御を実施すること。
 - (ii) 権限を与えられたContentsquareの担当者のみが顧客データにアクセスできるようにし、顧客データへの不正アクセス、破壊、又は紛失を防止するために商業的に合理的な措置を講じること。
 - (iii) (a) すべてのオペレーティングシステム及びアプリケーションに対するウイルス対策のアップデート、システムパッチ、修正及びアップデートの適時の適用、ファイアウォール及び顧客データの機密性、完全性、及び可用性を確保するために設計されたその他の同様の措置の実装、(b) 商業的に許容される暗号化ソリューションを使用し導入することにより、すべての顧客データを転送中及び保存中に常に暗号化すること、並びに(c) すべてのContentsquareドメインのための安全な電子メールの確保を含む、顧客データの安全な処理環境を維持すること。
4. Contentsquareは、顧客データが保護され、データ又はCSサービスが中断又は喪失した場合に、CSサービスの提供及び顧客データへのアクセスが復旧され、該当するサービスレベルで継続されるよう、事業継続計画を維持する。かかる計画は、経営陣によって見直され、承認され、毎年テストされている。
5. Contentsquareは、個人又は団体がコンピューター、システム、又はデバイスのセキュリティを回避し、顧客データの影響又はセキュリティ侵害(以下、個々に「インシデント」という。)をもたらしたと判断した場合、Contentsquareは、(a) 不正アクセスを直ちに終了させ、48時間以内に当該インシデントを書面で顧客に通知し、(b) 速やかに調査し、インシデントを是正するために合理的な措置を講じ、(c) インシデントの調査において顧客に協力し、顧客、又は法執行機関及び規制当局から合理的に要求される可能性のある文書と支援を提供するものとする。Contentsquareは、本マスターサービス契約の第11.10条に定める通知用のアドレス宛で、インシデントを顧客に通知するものとする。