

## 「HiConnex 情報セキュリティポリシー」

### (1) クラウドサービスの設計及び実態に適用する最低限の情報セキュリティ

社内で開発ガイドラインを整備し、それに則った開発を行うことにより、お客様に安定かつ安全なサービスをご提供しております。

### (2) 認可された内部関係者からのリスク

本番環境へのアクセスは、正当な理由が無い限りアクセスできない方針としています。

### (3) マルチテナンシー及びクラウドサービスカスタマの隔離(仮想化含む。)

当社クラウドサービスは、マルチテナントでサービスを提供しており、各社の IT リソースを論理的に分離しています。

### (4) クラウドサービスプロバイダーの担当職員による、クラウドサービスカスタマの資産へのアクセス

クラウド上のお客様データは、原則として弊社担当者が直接アクセスしないルールとなっておりますが、必要な場合にはクラウド利用者へ事前の承認を得るルールとしています。

### (5) 変更管理におけるクラウドサービスカスタマへの通知

2 週間前、1 週間前、当日、終了時に Web サイト上で告知を実施しております。

### (6) クラウドサービスカスタマデータへのアクセス及び保護

- ・お客様からの預り情報は、Microsoft Azure(「以下、Azure」)上で管理しております。  
当社クラウドサービス上に登録されたお客様データの処理や保管等は、Azure の ICT サプライチェーンの範囲に制限して利用しております。  
なお、データセンターの所在は日本国内です。
- ・暗号化技術の採用は、最新動向に着目し、安全性が評価されている技術を採用します。  
暗号化やハッシュ化によりお客様データを保護いたします。  
ユーザーのパスワードはソルト付きハッシュ化されております。
- ・当社クラウドサービスのセキュリティは Azure の不正アクセス防止機能により不正侵入が防止されています。
- ・当社クラウドサービス上に保管されたお客様データの消失、開示又は改ざんが発生するような障害、不正アクセス、  
又は、施設への不正侵入等の事象が発生した場合は即時管理者へ通知いたします。

### (7) クラウドサービスカスタマのアカウントのライフサイクル処理

お客様アカウントは、お客様自身で変更・追加・削除が可能です。  
詳細はユーザマニュアルをご参照ください。

**(8) 違反の通知、並びに調査及びフォレンジック(forensics)を支援するための情報共有方針**  
ログ情報のダウンロードまたは弊社(事業者)に依頼いただくことで調査を実施しております。

以上

2022 年 12 月 19 日制定