HITOTSU Link の情報漏えいリスクに関して

病院特化型コミュニケーションツール HITOTSU Link の導入検討に際し、情報漏えいのリスクに対する懸念の声がよく聞かれます。当社の考え方を以下にお示しします。

Q1. HITOTSU Link でのメッセージのやり取りが、ハッキング等で外部に漏えいしませんか？
A1. HITOTSU Link を開発・販売する HITOTSU 株式会社（以下、当社）は、2023 年 7 月、ISMS 認証を取得しています。ISMS とは、　　組織における情報セキュリティのリスクを管理する仕組み（体制やプロセス）のことで、国際規格を満たした ISMS を構築し、審査機関による審査に合格すると、ISMS 認証を取得できます。
詳細はこちら→「ISMS 認証「ISO/IEC 27001：2013」を取得しました」

- 参考）海外資本の大手チャットアプリでは、大規模な情報漏えい事案が発生し、複数回にわたり国の行政指導が行われました。情報セキュリティに関する安全管理措置の不備をめぐり、国レベルで問題となっています。

Q2. メッセージのやり取りを、HITOTSU が閲覧したり勝手に二次利用したりしませんか？
A2. 日本国憲法第 21 条第 2 項および電気通信事業法第 4 条に「通信の秘密」の保護が定められています。（ご参考→電気通信事業法及び通信の秘密（総務省 総合通信基盤局））
「通信の秘密」は憲法において厳格に保護されているものであり、当然ながら、当社はこれらの法令を順守し HITOTSU Link を開発・運営しています。安心してご利用ください。

また、当然、電気通信事業者の届出も行っています（総務省届出番号：A-05-20911）。電気通信事業法で義務付けられている外部送信規律も定め、法令を順守した開発・運営を行っています。

なお、HITOTSU Link 利用規約 第 4 条第 5 項においても、下記の通り規定しています（企業向けの HITOTSU Link for Biz 利用規約においても同様です）。

- 当社は、前項の個別のメッセージのやりとりに関し、メッセージの内容及び送受信の履歴を取り扱うに際して、HITOTSU Link ユーザの通信の秘密を守ります。なお、当社は、HITOTSU Link ユーザの同意に基づき、又は法令により求められ、若しくは法令により許容される限度において、HITOTSU Link ユーザのメッセージ等の通信内容や通信履歴を閲覧し、捜査機関や当局その他第三者に開示することがあります。

Q3. メッセージのやり取りが、競合他社に漏えいしませんか？
A3. HITOTSU Link では、トピックごとに「ルーム」を作成し、管理者が招待したメンバーがルームに加入することで、メンバー間のメッセージのやり取りが可能になります。
病院と企業とのルームには、病院ユーザーと当該企業のユーザーのみが加入できます。他の企業のユーザーには、ルームの存在は見えません。もちろん、ルームの内容（タイトル）やルーム内のメッセージのやり取り・添付ファイルも見えません。

ユーザーが故意にメッセージのやり取りを他社に漏えいしてしまうリスクは、電子メールや他のチャットアプリも含め、すべてのデジタルコミュニケーションツールに共通して存在します。また、紙による旧来型の情報共有に関しては、漏えいに加え、紛失や盗難のリスクもあります。メッセージの送信のたびに送信先を入力する電子メールに比べ、HITOTSU Link ではあらかじめ招待・設定したメンバー内でセミクローズドなやり取りを行うため、過失による漏えいのリスクは低いと考えられます。