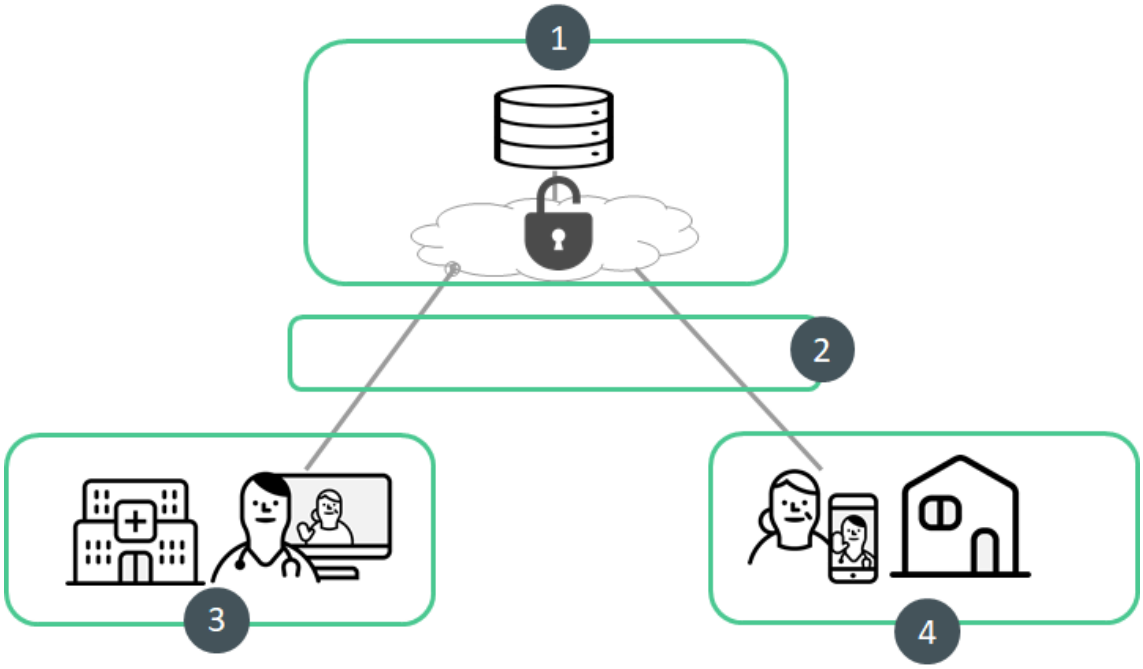
セキュリティ対応状況

YaDocは、安心して医療機関様、そして患者さんにお使いいただけるよう、高いセキュリティのもと、運用を行っております。



1: 堅牢なサーバ環境

信頼性の高いクラウドサービス（AWS：ISO 27001認証）を使用しております。
当社専任のセキュリティ管理者を配置し、WebサーバーおよびDBは、定期監視を行い、厳重に管理しております。

2: 通信の暗号化

サーバとユーザ間の通信は、ガイドラインで推奨されているSSL/TLS1.2を用いて、暗号化しております。これにより、第三者による盗聴や改ざんを防止しております。

3: ユーザ環境（医師）

御利用される医療機関ごとに、SSLクライアント証明書を発行します。
ユーザは、証明書をインストールした端末上で、IDとパスワードを入力してログインします。SSLクライアント証明書とログインID/パスワードの二要素認証により、セキュリティを高めています。

4: ユーザ環境（患者）

患者さんは、YaDocアカウント登録時に、登録したメールアドレスまたは電話番号への認証コードを発行して認証を行います。診療情報などのデータは、サーバ側で保管され、患者さんの端末には保存されないため、安心してお使いいただけます。

参考：厚生労働省 「オンライン診療の適切な実施に関する指針」への対応状況

（平成30年3月発行 情報セキュリティに関する指針）

ガイドライン要件		YaDoc対応状況
i）患者側の端末		
	患者の端末における適切な本人確認（認証）を実施すること （例）JPKIを活用した認証、端末へのクライアント証明書の導入 ID/PWの設定	✓ ID/PWによる認証を実施
	情報漏えいのリスクを軽減する観点から端末内にデータを残さないこと	✓ クラウドサーバへ保存
	端末へのウィルス対策ソフトの導入、OS・ソフトウェアのアップデートの実施を求めること（アップデートを行わなければ使用制限がかかる等） が必要である	- 動作環境について、最新OSを推奨
ii）オンライン診療システム・サービス		
	データをセキュリティ対策の行われた医療情報システム以外のシステム（患者・中間サーバー等）内に蓄積・残存させない。	✓ クラウドサーバへ保存
	システムの運用保守を行う医療機関の職員や事業者、クラウドサービス事業者におけるアクセス権限の管理（ID/パスワードや生体認証、IC カード等により複数要素の認証を実施することが望ましい。）	✓ ID/PWによる認証を実施
	不正アクセス防止措置（ファイアウォールや IDS/IPS を設置することが 望ましい。）	✓ 特定のポートのみのアクセス許可（ファイアウォール）とIDS(不正アクセスを検出する仕組み)を実施
	アクセスログの保全措置（ログ監視を実施することが望ましい。）	✓ 不正なアクセス兆候があった場合、ログを監視
	ウィルス対策や OS・ソフトウェアのアップデート	✓ クラウドサーバ上のソフトの更新は定期的に実施（緊急時はその都度）
iii）医師側の端末		
	医師の端末における適切な本人確認（認証）を実施すること （例）JPKIを活用した認証、端末へのクライアント証明書の導入 ID/PWの設定	✓ 医師側端末へのクライアント証明書の導入を必須とする ID/PWによる認証を実施

情報漏えいのリスクを軽減する観点から端末内にデータを残さないこと	✓	クラウドサーバへ保存
端末へのウィルス対策ソフトの導入、OS・ソフトウェアのアップデートの実施を求めること（アップデートを行わなければ使用制限がかかる等） が必要である	-	動作環境について、OS及びソフトウェアについて最新バージョンを推奨

iv）ネットワーク

信頼性の高い機関によって発行されたサーバ証明書を用いて、通信の暗号化（TLS1.2以上）を実施 または、特定の施設に継続的に接続する場合には、IP-VPNやIPSec＋IKEによる接続を行うことが望ましい	✓	通信の暗号化（TLS1.2）を実施