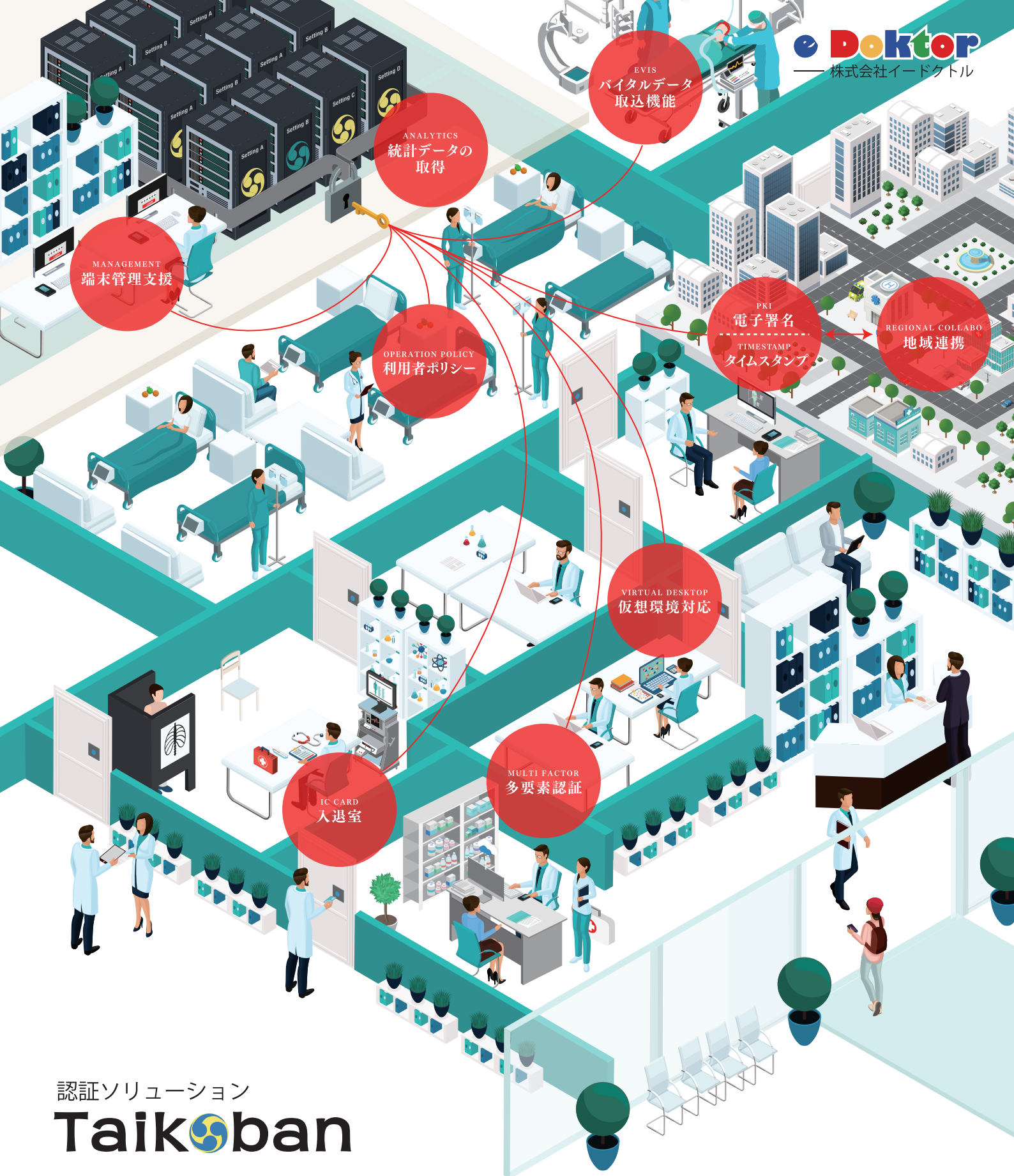




認証ソリューション

Taikoban

Taikobanは端末利用者の個人認証を行う為のシステムです。

端末利用時に  「いつ」  「だれが」  「どの端末を」の
3つの情報を収集すると共にWindows ログオンと同等のセキュアな環境を提供致します。

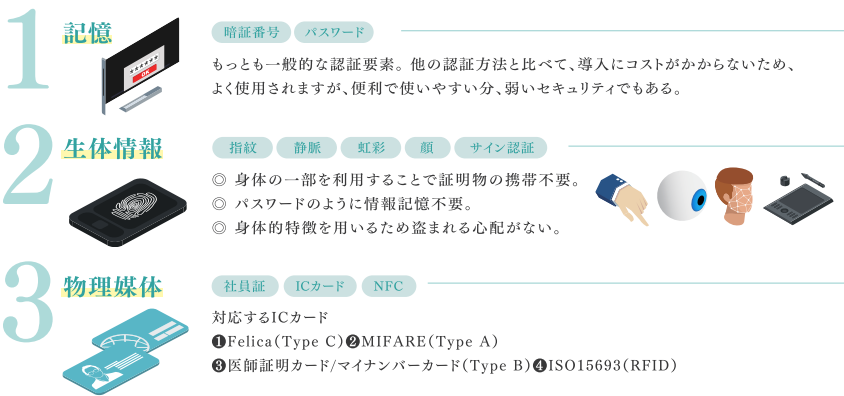
真正性を『担保する必要がある医療情報システム』では、IDとパスワードだけによる認証では脆弱です。

また、多数の部門システムが連携する医療情報システムでは、部門ごとにサインオン（ID＋パスワード）情報が散在してしまいます。

Taikobanは年々高度化・複雑化する医療情報システムに対し、簡単で安全、そして統一的な認証基盤を提供します。

組み合わせは様々。自由に選べる認証要素。

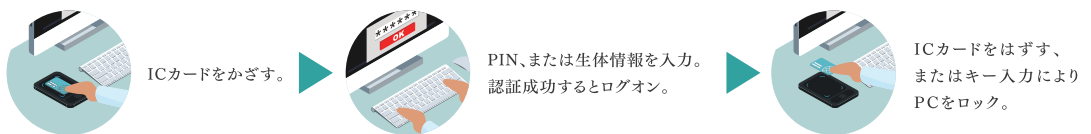
二要素認証は、これら3つの認証要素のうち種類の異なる2つの要素を組み合わせて認証する方式です。これによりセキュリティ強度が高まるため、なりすまし等の第三者による不正アクセスを防ぐことができます。



「記憶」「生体情報」「物理媒体」の組み合わせをユーザーの利用環境に合わせ、柔軟に対応いたします。



Taikobanによる一般的な認証フロー



Taikoban-SSO API

安全な認証・シングルサインオンを実現。

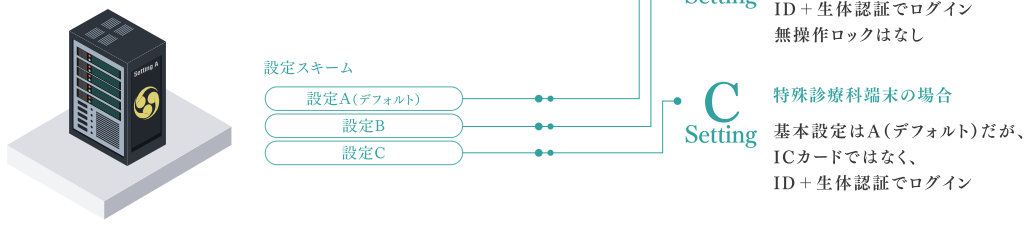
Taikobanのシングルサインオンはガイドライン準拠のエージェント方式を採用しています。各アプリケーションへの組み込みを可能とする「Taikoban SSO API」をご提供、各アプリケーションとの認証情報を連携させることにより、ログインの安全性を高めます。「簡単に」「厳密に」「共通に」認証を実現する基盤として提供します。



Flexible operational policy

柔軟な動作ポリシーの設定を実現。

高いセキュリティポリシーを設定すると、特定の人や部署では運用が行えず、利用者の利便性を低下させてしまいます。Taikobanは、高いセキュリティを確保した上で、利用者の利便性が損なわれないよう、部署や利用者ごとに動作ポリシーの設定・管理が可能です。



Enhanced security & high-speed user change

共有端末でのセキュリティ強化と高速ユーザー切替を実現。

病院情報システムで使用する端末の多くは、複数人利用を前提とした共有端末としてWindowsにログインしています。一方、個人アカウント運用の場合、ユーザー切替によるログオフ→ログオンの時間を要してしまうことが懸念されます。Taikobanは、共有端末での運用下でも個人アカウントと同等のセキュリティを確保し、さらに高速なユーザー切替・認証を実現します。

