

日々の業務で行われるファイルのやりとり

日々の業務内で、組織の内部・外部に関わらずファイルの共有は頻繁に行われます。その一方で、病院様では患者様の個人情報を含む重要なファイルを多く取り扱ってられるため、セキュリティ対策講じたシステム運用が求められています。

その為、一般的に病院様ではインターネットへ接続できる環境と、組織内の機密情報等を扱う環境はネットワークレベルで分離させています。これは情報漏洩やセキュリティリスクの対策に効果的であり、インターネット利用の安全性を向上させます。

しかし、業務上の課題もあります。

組織内のファイルを利用して業務を行う場合、



- ① ファイルを組織外の人へ共有したい
- ① インターネット上でファイルを使用したい
- ① 家で作成した資料を持ち込みたい
- ① USBメモリーを使用させたくない

このように、安全性を向上させる為の仕組みによってファイルの持ち出しや持ち込みを制限され、結果的に業務の利便性が低下してしまいます。

ファイルのやり取りの定番 Fit Smart Trans

Fit Smart Transは、以下の機能によりファイルやりとりにおける課題を解消いたします。

ファイルの送受信履歴を管理

- ▶ アップロードもダウンロードも、Web画面上でのシンプルな操作で実施可能
- ▶ 送受信履歴の管理をブラウザ上で行うので、異なるネットワーク間のファイルのやり取りも安全に行うことができます。

ダウンロードするファイルの承認機能

- ▶ ファイルのダウンロードの際に申請を行う運用が可能です。その場合、管理者(上長)はユーザーからの申請に対し承認または却下の処理を行います。
ダウンロードの申請が却下されたファイルはダウンロード出来ません。

転送履歴と転送ログなどの証跡ファイルはサーバー内に保存

- ▶ ユーザーが行った転送について詳細を転送履歴に記録します。転送履歴は管理者用のページで確認が可能です。
- ▶ 証跡ファイルはサーバー内のフォルダに日付単位で保存されます。

電子カルテと連携可能

- ▶ ログイン認証に電子カルテのユーザー情報を利用することができます。

〒532-0011

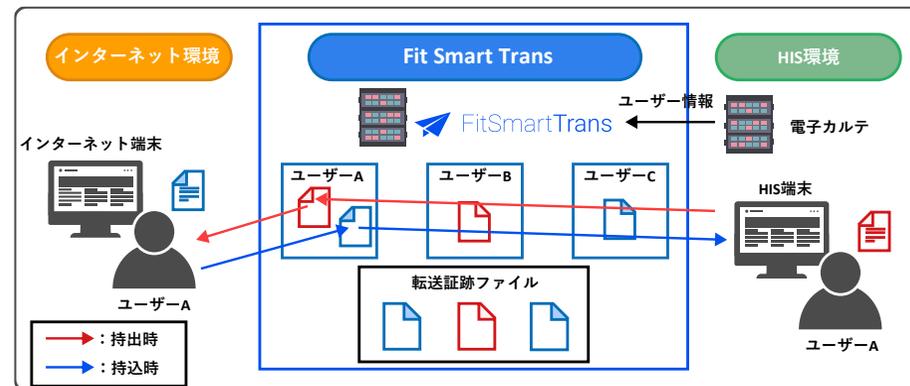
大阪市淀川区西中島6-11-25 第10新大阪ビル

TEL.06-6889-5777 FAX.06-6889-5778

sales@fit-works.co.jp

システム概要

ブラウザ上のFit Smart Transからアップロード処理を行ったファイルは、ファイル転送サーバー(Fit Smart Trans)上にアップロードされます。ファイルのダウンロードは上長に申請を行い、承認が下りた場合のみ可能とする運用も出来ます。また、ログイン認証には電子カルテのユーザー情報が利用出来ます。



オプション製品との連携で、よりセキュアに。

個人情報チェックやウイルス対策オプション製品との連携を行い、よりセキュアな送受信を行うことが出来ます。

HIS系ネットワークからのファイル持ち出し時には個人情報のチェックを行い情報漏えいの防止を、HISネットワークへのファイル持ち込み時にはマルチスキャンエンジンで検疫してウイルスチェックを行い、セキュリティをより強固なものにします。

