

安全な情報共有のためのプラットフォーム “働き方改革”を支える クラウドファイルサービス



会社の元気を支える柔軟で自由な働き方、でも情報の取り扱いが安全に。

既存のファイルサーバーのように全社の集中管理と柔軟な権限管理をSaaSのストレージサービスで実現！

企業にとっての“働き方改革”とは？

昨今話題の“働き方改革”とは、ワーカーの多様性への対応や時間や場所、チーム、個人等の制約を受けない業務環境の整備による、生産性の高いリソースの確保のための取り組みです。これにより、健康で幸せに働くスタッフを増やすことはもちろん、最終的には企業としての価値の向上とビジネス拡大を目指す必要があります。改革は一日にして成らず。企業には、新しいビジネス基盤と仕組みの整備への第一歩が求められています。



“働き方改革”担当部門はどこから着手すべき？



「人（ワーカー）の管理」から「仕組みと成果の管理」へ

組織における意識改革や社内制度の策定においては、「人（ワーカー）の管理」から「仕組みと成果の管理」へシフトしていく必要があります。ここでいうビジネス基盤として重要なのは言うまでもなくICTの活用です。経営者を含めた意識の変革も必要ですが、安全で効率的に業務を行えるICT環境を整備しないことには、全社で統一された意識の醸成や仕組みの定着は難しくなります。

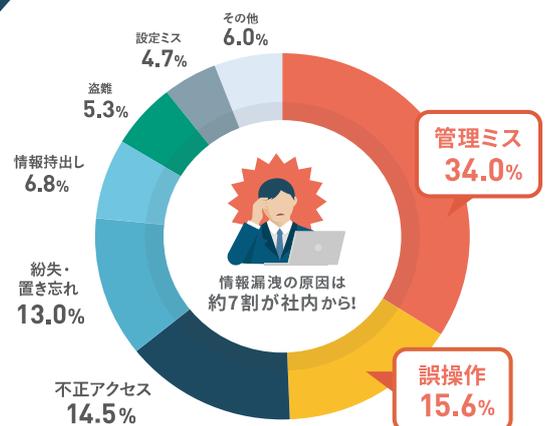
ICTでセキュアな情報共有基盤づくり

社内外との安全な情報共有プラットフォームを構築するには

多くの企業にとってテレワーク導入の一番の懸念は「情報漏えいリスク」です。企業の情報漏洩インシデントの約7割が社員の不注意、過失、故意のデータ持出しが原因となっており、外部からの攻撃より圧倒的に多いのです。より詳しく原因を見ていくとメール添付によるファイル共有時の誤操作による情報漏えいや、個人の判断で利用しているクラウドサービスの社内データ保管場所を、管理者が把握できていないことがそのリスクを大きくしています。テレワークのメリットを得るためには、リスクを恐れるだけではなく、ユーザーや管理者にとって「わかりやすく使いやすい情報プラットフォームとしてのファイルサービスの構築が必要です。

ユーザーリテラシーに依存せず、企業主体のセキュアな仕組みづくりで情報漏えいを防ぐ

現在のファイルサーバーの運用において、各ワーカーのアクセス権は適切に管理をされているでしょうか。また、ファイル共有の方法としてパスワードが徹底されていないメール添付や各個人で使っているUSBやセキュリティ面での確認がされていないB2C向けのWebサービス（シャドーIT）が自由に利用されていませんか。それぞれのワーカーが必要な情報にだけアクセスできる権限を付与し、適切なメンテナンスを継続できること。そして、社内外とのファイル共有方法をシステム面と運用面でしっかりと組織内で統一されたルールを作る。クラウドサービスの選定時にも間違いやうっかりミスは発生する前提で「安全な仕組み」をしっかりと管理できるものを選ぶことが情報セキュリティのキープポイントとなります。



【出展】「2016年情報セキュリティインシデントに関する調査報告書」
NPO日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ

POINT 情報セキュリティのポイント

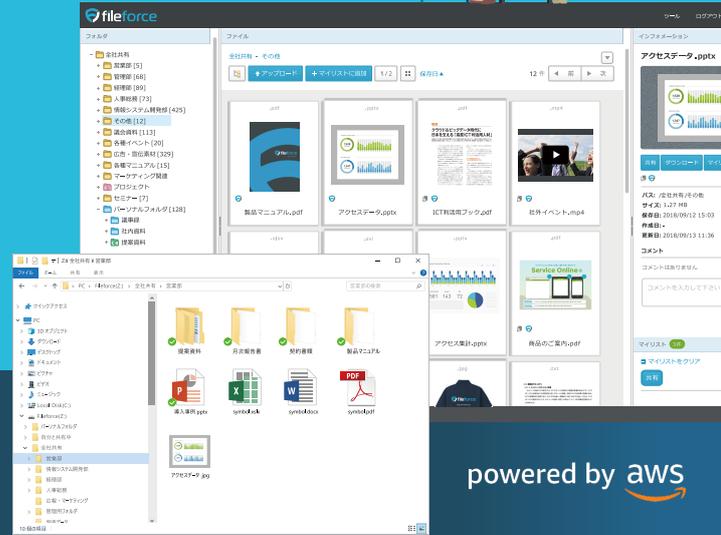
- 01/ 業務に必要な情報にのみアクセスできる柔軟な権限管理ができる仕組みを構築することで、企業として社内データの中央・集中管理を行える環境を作る
- 02/ ファイル保管先や社内外とのファイル共有方法の統一とその証跡を確実に管理する

クラウドで実現する セキュアな テレワーク環境



Fileforce®は既存ファイルサーバーの運用を変えない柔軟な権限管理と優れた使い勝手を実現したクラウドファイルサービス。企業の規模・業種・業務を問わず効率的な働き方を支え、パフォーマンスを高めます。

- ✓ ストリーミングで通信コストを削減
- ✓ ローカルディスクを圧迫しないキャッシュ機能
- ✓ オフライン利用も可能

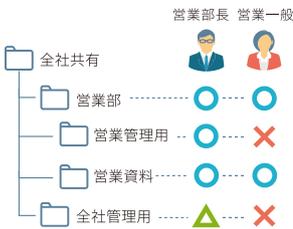


powered by AWS

組織に合わせた柔軟な権限コントロール

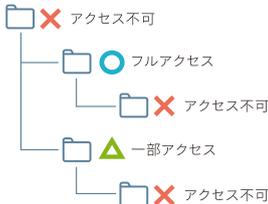
柔軟なアクセス権限設定

上位の権限を継承をするだけでなく、部署フォルダ内に管理職ユーザーのみアクセスできるフォルダを作る等、限定的な利用も行えます。



制約のない権限の継承

階層や相互位置関係に制限されず任意のフォルダや階層で権限の継承を柔軟にコントロール。フォルダ内でアクセスできるユーザーを絞り込む事も可能です。



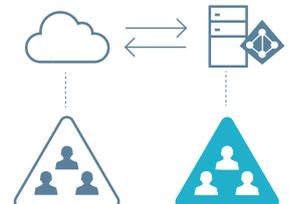
アクセス許可項目を組合せ

20以上の項目を組み合わせてアクセス権限を柔軟にカスタマイズ可能。独自のニーズに合わせた権限設定が可能で既存のアクセス権限も踏襲できます。



Active Directory 連携

ユーザーやグループ情報は管理ツールでの設定のほか、Active Directoryとの連携も可能。権限管理の負担を大幅に軽減します。



場所を問わない情報共有を支援

すべてを証跡として記録

管理者も含めたユーザーの操作履歴やファイル共有の状況、アクセス履歴など情報を全て記録しています。



承認ワークフロー機能

共有リンクを発行する際に上長の承認を取るプロセスもシステム化が可能です。



社外ユーザーとの共有

アカウントを持たないユーザーとも、権限の割り当てにより安全にファイルの共有が行えます。



IPやマップなど多彩な認証

パスワード、IP制限や、位置情報によるマップ認証があり、レベルに応じ自由に組み合わせが可能です。



その他のセキュリティ機能

- ✓ ユーザーの操作をログとして記録
- ✓ 保管時に自動でウイルスチェック
- ✓ データの更新時に自動的に保存
- ✓ シングルサインオン(SSO)標準対応
- ✓ ファイルの変更履歴を保存
- ✓ 通信経路・保管データの暗号化
- ✓ 各種ポリシー設定
- ✓ 開発も保管場所も国内だから安心