ファイルプロテクション機能について

TotalFileGuardの主要な機能の「暗号化」についてご説明いたします。

■ 暗号化

●TotalFileGuardの基本的なコンセプト:

ユーザが意識せず自動暗号/復号化を行うファイルプロテクション

・暗号化は素早く、復号化は直前に
平文のままファイルが存在している時間が長いほど、漏洩の危険性が高くなります。TFGではファイル作成後自動的に暗号化し、ファイル展開時に自動的に復号化して保護します。

・操作手順は変わらずに、プロテクトは確実に
通常の手順と変わった操作をさせることは操作ミスを誘発します。慣れた操作でありながら確実な保護を行うことで誤操作などによる漏洩を防ぎます。

・管理は簡単に、操作ログは忠実に
管理者にとって運用管理は想像以上に負担になります。また管理者権限の悪用に対しては管理が難しいものです。運用管理を容易にし、管理者の操作履歴を確実に記録できることで、確実な運用を可能にします。

・習得時間は短く、インストール作業は速やかに
堅固なツールでも操作方法を誤ると効果がありません。TFGでは分かりやすく簡単な操作方法で運用可能です。またシステムの構築も容易に行えます。

■ TotalFileGuardで保護するファイルを設定する方法

・アプリケーション単位での保護
ファイルを暗号化して保護したいアプリケーションを登録します。登録されたアプリケーションのファイルは利用時に全て暗号化されます。

・拡張子単位での保護
拡張子を指定してファイルを暗号化します。クライアントプログラムが定期的にPC内をスキャンし、指定された拡張子を全て暗号化します。

※操作したファイルは場所に関係なく全て暗号化
ファイルを開いた場所がクライアントプログラムをインストールしていないファイルサーバ上に保管されていても、インストール済みPC上で操作された場合には全て暗号化されます。

■ 復号化

・復号化できる条件
・クライアントプログラムがインストールされている
・管理サーバと接続している
・認証が行われ許可される
・情報管理者から権限が付与されている
・管理者から許可される
上記条件を最低一つ以上クリアしなければ復号化ができません。

・様々な認証方法で利用環境に左右されない
復号化可能条件のうちもっとも基本的な「認証」の方法は以下の四通りになりますが、それぞれに複数の手段を用意しています。ファイルを利用する機会に支障が出ないよう、柔軟な対応が可能です。
・管理サーバによる認証 - アカウントやクライアントPCのHDDを認識、またUSBトークンを併用して認証等を設定可能です。
・USBトークンによる認証 - アカウント・パスワードによる認証、管理サーバによるHDDの認証、等を設定可能です。
・ソフトウェアによる認証 - トークンキーや管理サーバとの接続に影響されない特殊な認証方法です。
・事前の情報管理者からの許可による認証 - 特別な権限による復号化権限を付与することが可能です。

・権限設定で復号化の制限も可能
認証され復号化可能な条件を満たしたとしても、安易な復号化を避けるためにファイルを復号する際に管理者承認を必要とすることが可能です。この場合、管理サーバとオンラインである必要があります。

■ TotalFileGuardでの復号化とは

・一時的な復号化
TFGで暗号化されて保管しているファイルを修正・変更・印刷等の操作を行う目的で使用可能な状態にすること。操作終了後再度ファイルを保管するために「閉じる」操作を行うことで自動的に暗号化ファイルへ戻ります。

・常時的な復号化
TFGのクライアントプログラムがインストールされていない環境へファイルを提供するような際に、一般的に閲覧可能な状態にすること。TFGのクライアントプログラムがインストールされていないPC上では通常のファイルと同様に使用できます。

運用管理

TFGを有効的に運用するため、様々な機能が利用可能です。

管理センター

TFGの運用管理を一括して行う管理ツールです。主に以下の機能が利用できます。

・エージェント作成、アップロード、ポリシー設定/変更
クライアントPCを制御するエージェントを管理センターで作成します。エージェントがインストールされたクライアントPCは管理センターから様々な管理を行うことができるようになります。

・ログの閲覧/監査
クライアントPC上の操作、及び管理者の操作を記録します。管理センター上からログのバックアップが実行できます。また、バックアップされたログを復元して管理センター上で監査することも可能です。

・USBトークンキーの作成、パスワード設定
クライアントPCの認証に係るUSBトークンキーや、アカウント・パスワードの設定・変更が可能です。

・メッセージの送信、各種権限の付与
クライアントPCへのメッセージ送信、リモート操作が可能です。メッセージ送信時にオフラインのクライアントPCには、次回オンライン時に自動送信します。

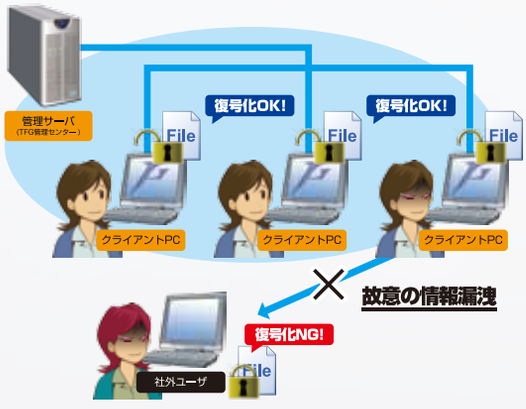
・管理クライアントPCの管理、TFGシステムの管理
システムの健全な運用を実現するために、システム全体のメンテナンス、クライアントPCの状態確認が行えます。

エージェント(クライアントPCにインストールされるプログラム)の作成・ポリシー(制御の詳細な設定)の設定

管理者によって作成されたプログラム(エージェント、ポリシー)を各クライアントPCへリモートインストールできます。

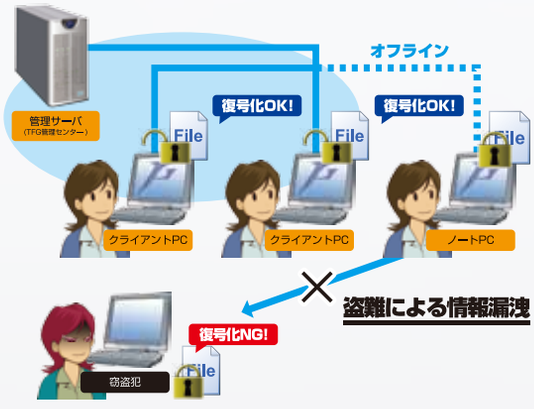
運用事例

運用事例1 社内の機密データの流出対策や知的財産権の保護として



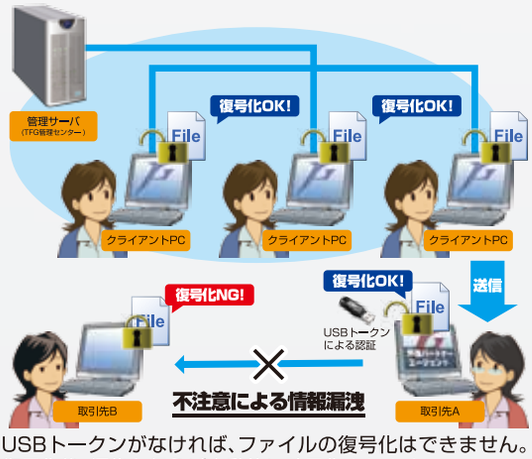
TotalFileGuardがインストールされていなければ暗号化ファイルを復号化できません。

運用事例2 ノートPCの盗難、置き引き対策として



USBトークンによる認証にしておけば、ノートPCの盗難対策としても安心です。

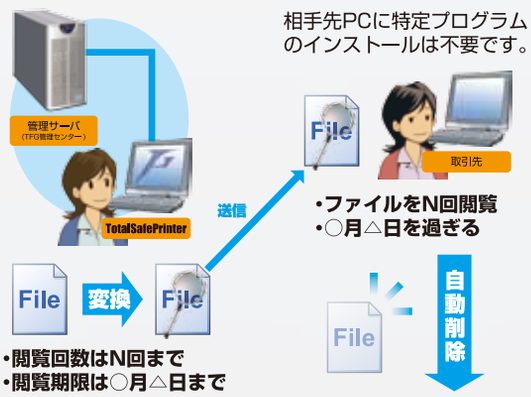
運用事例3 取引先企業との大切なデータのやり取りに(取引先で編集可能)※1



USBトークンがなければ、ファイルの復号化はできません。
復号化後、編集を行えば自動的に暗号化されます。

※1P.7:外部パートナーエージェントを参照してください。

運用事例4 取引先企業との大切なデータのやり取りに(取引先で閲覧のみ)※2



TotalSafePrinterで
ファイルを閲覧専用
ファイルに変換します。

ファイルは自動的に削除されます。
ゴミ箱にも残りません。

※2P.3:TotalSafePrinterを参照してください。