

情報セキュリティ 【製造業編】

ファイル暗号化運用で技術情報を守る

CAD で作成した図面ファイルを暗号化して守りたい！

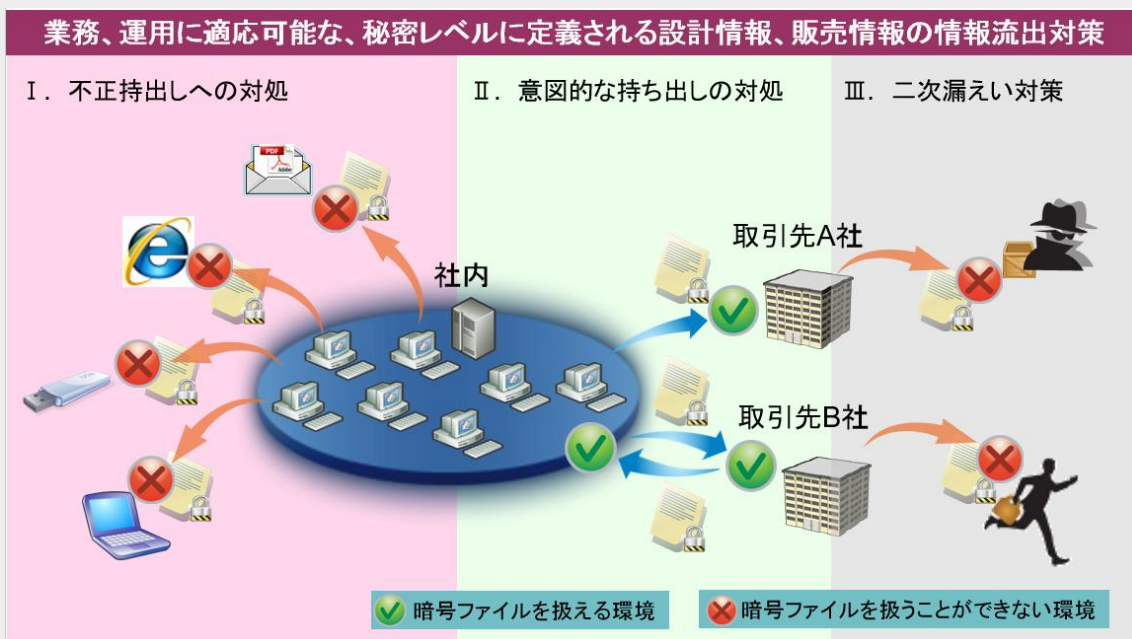
- ～ どこまで守れる？
- ～ ファイル暗号化製品をどう選ぶ？



1. ファイル暗号化技術の利点

製造業のものづくり現場は一般企業の業務と異なり、特殊なアプリケーションを使って製品の設計を行ったり、設計図面を社外に持ち出してお客様との打ち合わせで使用したり、外注先に図面を渡して部品を加工してもらったりと、「ものをつくる」ために、製品情報が社内外のあらゆる場所で扱われている。製造業では、このような業務の運用を考慮して製品情報を守らなければならないのだが、それぞれの業務の運用の中に潜む脅威は次の3つに大きく分類される。

- ① 不正持出し
- ② 意図的な持出し
- ③ 二次漏えい



3つに分類される脅威に対して、それぞれに合ったセキュリティ対策を行っていくことも一つの手段ではあるが、できることなら3つの全ての脅威を1つのセキュリティ対策で対応できるのが望ましい。そこで注目したいのが「ファイル暗号技術」である。ファイル暗号技術を使えば、守りたい情報ファイルを暗号化して、社内外の端末で暗号ファイルを復号することなく扱うことができれば、万が一暗号ファイルが想定外に流出されて想定されていない端末で暗号ファイルが扱われようとしても、ファイルが開かないことでファイル内の情報が守られるという理屈になる。

つまり、ファイルが流出されることを前提に、誰にファイルが渡っても、把握されている許可された端末でしかファイルを開くことができないという環境を作り運用することで、ファイルに書かれた情報が守られることになる。このような運用を「ファイル暗号化運用」という。

2. ファイル暗号化運用に必要なファイル暗号化製品の機能と特長

透過式ファイル暗号化機能

透過式とは、アプリケーションでファイルを作成したタイミングからファイルを削除するまでの間、ファイルを復号することなく暗号化された状態を維持しながら、アプリケーションで利用可能なことをいう。ファイルを暗号化することはできても、暗号ファイルを暗号化したままアプリケーションで開いて扱うことは技術的に難しいが、安易に復号してアプリケーションで扱うようなことをすると、復号されたファイルが一時的に存在することになり、情報漏洩を引き起こしかねない。従って、一時的にも復号するのは運用で避けるべきであり、一度暗号化したファイルを復号することなく、運用で扱っていきける透過式ファイル暗号機能が必須となる。

アプリケーション対応

MS Office、Adobe PDF 以外のアプリケーションにも対応できる機能が必要。製造業では、特に CAD アプリケーションの対応が必須となる。また、アプリケーション対応で特に重要なポイントは、アプリケーションで「ファイルを保存」や「エクスポート」でファイルが自動的に暗号化され、アプリケーションで「ファイルを開く」や「インポート」で暗号ファイルが開けるようにしなければならない。

オフライン認証機能

一般的にファイル暗号化製品の認証方式は、認証サーバと端末間でオンライン認証をする仕組みとなっている。オンライン認証は社内の端末であれば有効だが、社外の端末で特に取引先や外注先の別会社の端末を想定した場合、社内の認証サーバと別会社の端末をオンラインで接続できる環境は簡単に提供できない。オフライン認証機能は別会社に重要なファイルを渡して、別会社の許可された端末上のみで扱うことができるようにするために重要な機能となる。

中国利用

国内のファイル暗号化製品の中では、中国で利用できる製品は少ない。その反面、多くの製造業のセキュリティの課題は中国にある。海外生産する場合に海外に図面を出さなければならないが、特に中国に図面を出したときの二次漏洩が心配という企業が多い。せっかく国内でファイル暗号化製品を導入しても中国に暗号ファイルを出すことができないとなると目的を達成できない。対中国の二次漏洩対策が目的であるなら、まずは中国の商用暗号管理条例に違反しないファイル暗号化製品を選択しなければならない。

印刷制御

ファイルが暗号化されていても、暗号ファイルを扱う権限のある人がアプリケーションで印刷して、情報を紙の状態を持ち出すことも想定しておかなければならない。また仮想印刷のように、ファイルを変換して異なるファイル形式のファイルとして保存もできるため、このような操作を制御する必要がある。

画面キャプチャーとクリップボード制御機能

ファイルが暗号化されていても、暗号ファイルを扱う権限のある人がアプリケーションで暗号ファイルを開き、プリントスクリーンやスナッピングツールなどで画面イメージをファイルにされることを想定しておかなければならない。また、誰もが常日頃行っている操作である「コピー | 貼り付け」もセキュリティの観点で見ると、とても危険な操作である。これらの操作によって、新たに作られたファイルが暗号化されずにそのまま持ち出されたら情報が流出される結果となるため、画面キャプチャーとクリップボードの制御は必要に応じて行う必要がある。

ファイル容量の増加とファイルを開く速度遅延

もともと暗号化されていないファイル（平文）と同じファイルを暗号化したときの暗号ファイルを比較すると、当然のことながら暗号処理されたファイルの方が、情報量が多くなることによってファイル容量が増えることになる。また、暗号ファイルをアプリケーションで開くときに、ファイル暗号化製品の仕組みの中でファイルを一端内部的に復号（復号されたファイルは存在しない状態）してアプリケーションにデータとして渡してメモリに展開している。その際の内部的な復号処理がファイルを開くときのオーバーヘッドとなることがある。ファイル暗号化製品の中では、暗号ファイルを開く速度が平文と比べて2倍もかかるようなこともある。一般的なアプリケーションでは作られるファイル容量は小さいが、CADのようなアプリケーションでは一つのファイルが数百MBになることもあり、数百MBのファイルを開くのに1分かかっていたものが、そのファイルを暗号化したことで2分以上待たなければファイルが開かない事態に陥ることがある。ファイル容量の増加とファイルを開く速度もファイル暗号化製品を選ぶ場合の重要なポイントとなってくる。

申請機能

重要な情報ファイルを透過式ファイル暗号化機能で守り続けながら仕事で扱うことが最善ではあるが、時には一時的に暗号ファイルを復号しなければ業務が回らない場合も想定しなければならない。その場合の復号方法も良く検討する必要がある。安易にユーザに自己復号権限を与えたのではファイルを暗号化している意味がなくなる。多くのファイル暗号化製品には、一時的に暗号ファイルを復号するための復号申請機能を持っている。この申請機能を使うことで、ユーザ自身が自由に暗号ファイルを復号するのではなく、必ず管理者や部門の役職者に復号申請を上げて承認を得ないと復号できないという運用が可能となる。また、ユーザが「いつ」、「何の暗号ファイル」を、「どういう理由」で復号したいのか？承認者が「いつ」申請を「承認 | 否認」したのか？をしっかりとログとして取っておく必要がある。このような申請機能は、ファイル暗号化運用の中で仕事を進めるために必要となる場合がある。

ユーザに与える影響

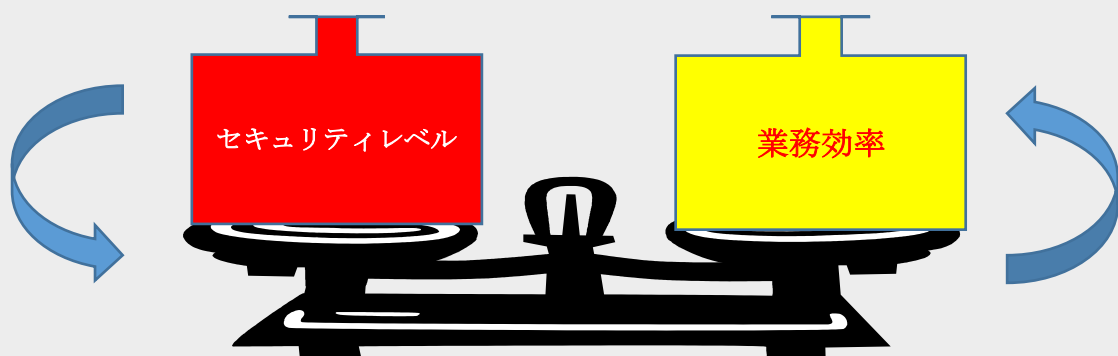
ファイルの圧縮解凍ツールのように、圧縮したいファイルを選択してマウス右ボタン操作で圧縮を実行するような操作を、ファイルを暗号化するためとは言え、ファイルの「新規保存」「上書き保存」「エクスポート」の後に、同じような操作感で、作ったファイルに対して暗号化を実行するようなことはユーザの負担が大きく、フラストレーションもたまり、時間とともに暗号化操作をやらなくなる。ファイル暗号化製品の中には、ファイルを暗号化する際にユーザに暗号化操作をやらせる製品もある。最も多いのが、ファイル暗号化製品内で設定しているファイルパス（フォルダ）にファイルを入れることで自動的に暗号化処理が実行されるといった機能になる。また暗号ファイルをアプリケーションで開くことができなくて、ファイルを開く前に対象ファイルを復号するような製品もある。その場合の復号操作でよく使う。

3. セキュリティ強化と業務効率

当然のことながら、セキュリティ対策を強化するということは、これまで普通に行っていた操作や使えていた機能が制限されることになり、作業効率が低下することは否めない。製造業にとっては、会社のコンプライアンスに関わるセキュリティ対策も非常に重要なことではあるが、作業効率の低下により製品の開発スケジュールの遅れ、生産スケジュールの見直し、さらに発売時期の遅れや出荷時期の遅れにより注文のキャンセルや競合他社に先を越されて顧客を取られることもあり、結果として会社の売り上げに影響する事態になることも少なから

ずある。ファイル暗号化運用における最も重要なポイントは情報を漏洩しないように守ることではあるが、同じレベルで業務効率を低下させないことである。ファイル暗号化製品を選択する場合、先に述べた製品の機能や特徴も吟味する必要はあるが、合わせてセキュリティレベルを上げることで、業務効率がどこまで維持できるか、これまでの業務がどう変わっていくのかを見極めておかなければならない。

セキュリティレベルと業務効率はトレードオフ



セキュリティ対策の一般的なご質問から各種セキュリティ製品に関することまで、何でもお気軽にお問い合わせ下さい。これまでファイル暗号化によるセキュリティ対策支援を約7年経験し、大小問わず多くの企業様に販売実績を持つピコテクノロジーズ株式会社がお答えします。また、製造業のものづくりを熟知したセキュリティアドバイザーが、ものづくり現場に特化したセキュリティ対策のアドバイスも行っております。

ピコテクノロジーズ株式会社

☎ 03-6403-0906

Mail : info@pico-t.co.jp

Web サイト : <https://pico-t.co.jp/contact/>