

ファイル送信者ツールでは解決できない 受信側のセキュリティリスク

インターネットでファイルを送受信する場面に於いては、送る側が利用する「ファイル送信者ツール」を使って送る方法と、受け側が利用する「ファイル受信者ツール」を送る側へ提供して受け取る方法の、二種類の方法があります。

1. ファイル送信者ツール

ファイルを送る側が利用するサービスで送信する、送信者主導のサービス

- ① PPAP 送信
- ② ファイル送信 (WEB アップロード型) ... ファイル送受信に特化したサービス
- ③ クラウド送信 (URL 送信型) ... クラウドサービスの拡張
- ④ ファイル送信 (メール分離型) ... メールからファイルを取り出し
WEB などへ保管し、URL を送信

「PPAP」を除く、これらサービスでは、

- ❑ 送信時に 2 段階認証や、2 要素認証などで不正利用をされない
- ❑ 操作ログが詳細に取得できる
- ❑ 送信時に上長の承認が取れる

などをもって、送信時のセキュリティが充実していて、安心して利用できると言われています。

確かに送信システムを第三者に悪用されない為には、認証機能を充実させることが必要で、不正利用のチェックには操作ログの解析も有効です。また、上長の承認を取ることで、間違った内容や違う相手に送ってしまうことを未然に防ぐことができます。

しかし、それらは全て、送信者側の問題だけを解決するものでしかありません。

前記の様な充実したセキュリティ対策がなされているサービスを使って送られたファイルならば、躊躇せずに 100% 安心して受信して良いのでしょうか？

もし、本物そっくりに模倣された「WEB サービス」が用意されて、本物そっくりに記載された「ファイルの送信通知」を受け取った場合、その通知がなりすまし送信されたものであっても、偽物に気が付かず、あたかも本物のサービスから届いたかの如く受け入れてしまい、結果、様々な脅威に直面することはないのでしょうか？

「偽の WEB サービス」を開設することも、「偽のファイル送信通知」を送り付けることも容易であり、それらの行為を誰も妨げることができません。

銀行やクレジットカードの認証情報を盗みだす目的で、本物そっくりの偽サイトを使ったフィッシングの手口は既に当たり前となり、企業への標的型攻撃を考えると、今後、ファイルの送受信に関係したサービスの模倣も進むものと思えるのは、ごく自然な流れです。

ゆえに、送信者主導サービスの様々なセキュリティ対策は、送信時には有効でも、受信者側からしてみれば、完全に信頼するには足りない内容だと言えます。

2. ファイル受信者ツール

ファイルを受け取る側が利用するサービスを送る側へ提供して受信する、受信者主導のサービス

⑤ ファイル共有(クラウド共有)

「ファイル共有(クラウド共有)」の特徴としては、

- ❑ 許可された送信者だけが利用できる、なりすまし送信されない
- ❑ 送信者毎に認証情報と共有領域を管理する
- ❑ システムを利用して送信できる権限を、送信者へ貸与する
- ❑ 権限を貸与された送信者は、厳重な管理を要求される

となっていて、信頼関係のある取引先との間での利用に限定されます。

安全にファイルを受け取れますが、送信者毎に認証情報や共有領域の管理が必要で、慎重な運用が要求されます。

取引先からのパスワード流出や、環境設定の誤りが、情報漏えいリスクにつながることへの注意も必要です。

3. 新しいファイル受信者ツール

新たな手順でファイルを受け渡しする、受信者主導のサービス

⑥ RSF ファイル交換サービス(SafetyCarrier)

「RSF ファイル交換サービス(SafetyCarrier)」の特徴としては、

- ❑ 自分のメールアドレスを使っていれば、誰からでも利用できる
- ❑ なりすまし送信されない
- ❑ 受け取りを許可していない送信者からの受信に、警告または、拒否ができる
- ❑ 認証情報は交換しない
- ❑ ファイルは共有せず、送信者毎の環境設定作業も必要ない

誰とでもファイルの交換ができ、パスワードなどの認証情報の交換も不要、環境の設定も必要ありません。

許可のない送信先からの受け取りを拒否することで「ファイル共有(クラウド共有)」と同様に、信頼のある取引先からだけファイルを受信する運用もできます。取引先の管理は、送信者アドレスを許可するだけの作業となり、完全に受け取り側だけの管理でファイルの送信相手を限定する運用が可能となります。

ファイル送信者へメールを送り返すことが、なりすまし送信への防衛策となります。

そして、正確な送信者アドレスの獲得が、なりすましされていない正しいアドレスを使った許可リスト(ホワイトリスト)の構築へとつながり、まぎらわしいアドレスを使った送信者のチェックアウトを確実にし、フィッシング送信を暴いて警鐘を発することにつながります。

RSF ファイル交換サービス(SafetyCarrier)は、ファイルの受信者を守るサービスです。