取引先に限定してファイルを受け取る

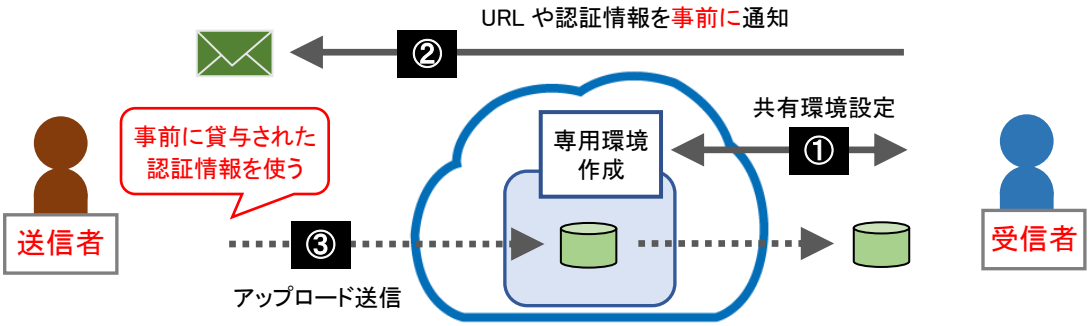
サプライチェーンのリスクを軽減、取引先に負担をかけない

クラウド共有を使うと、取引先から安全にファイルを受け取ることができます。取引先へクラウドへアクセスする為の認証情報を事前に渡すことで、許可のない第三者からのファイル送信を防ぎます。しかし、取引先への認証情報は事前に貸与しておくことが必要で、取引先では預かった認証情報の厳重な管理を求められます。
また、クラウド共有の場合、ファイルの受け渡しに利用する領域は、送り側と受け側の両方がアクセスできる領域を恒常的に確保するのが一般的で、**共有領域のアクセス権の管理**に注意が必要です。設定を誤ると、社外秘の情報が漏えいするなど、重大な事故につながる危険をはらんでいます。また、取引先でのセキュリティインシデントの発生が、自社へ影響するなども想定した対策が必要です。

本書では、RSF ファイル交換サービス - SafetyCarrier を使うと、限定した取引先だけと安全で手軽にファイルを受信できる環境が構築できることを紹介します。

1. クラウドストレージ共有を使ったファイルの受け取り

事前にファイルを受け取る側が送る側に URL や認証情報を貸与し、送る側は貸与された URL や認証情報を使いファイルをアップロードして送信します。

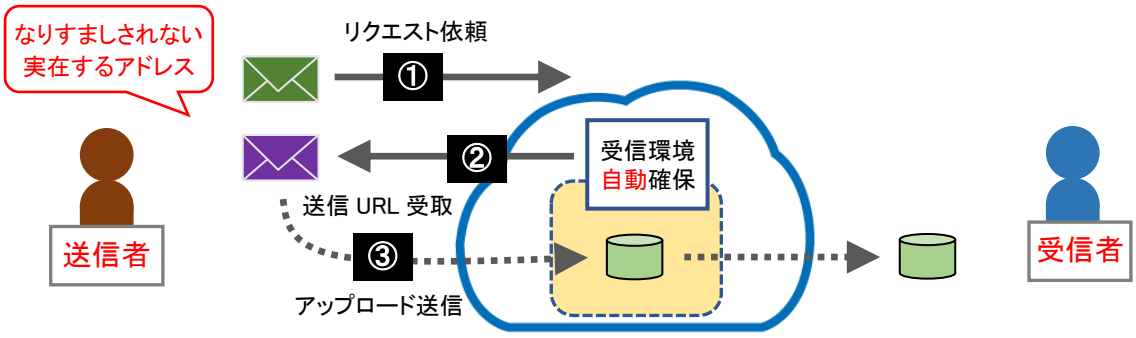


ファイルの受信者はファイルの送信者専用の共有領域を用意し(①)、事前にファイルの送信者へ URL や認証情報を貸与します(②)。
ファイルの送信は、貸与された URL と認証情報を使ってファイルをアップロードします(③)。

特徴としては、ファイルの送信者へ貸与された認証情報は厳重な管理が要求され、送信者側のセキュリティインシデントが発生した場合には、受信者側へ被害が及ぶことも考えられます。
また、共有領域の設定ミスから意図しないファイルやフォルダーへの閲覧を許してしまうことにも注意が必要です。
この様に、**共有領域の厳格なアクセス権管理**作業が発生するだけでなく、自社の努力の及ばない**取引先での事故にも影響を受ける**などの点も考慮しないとなりません。

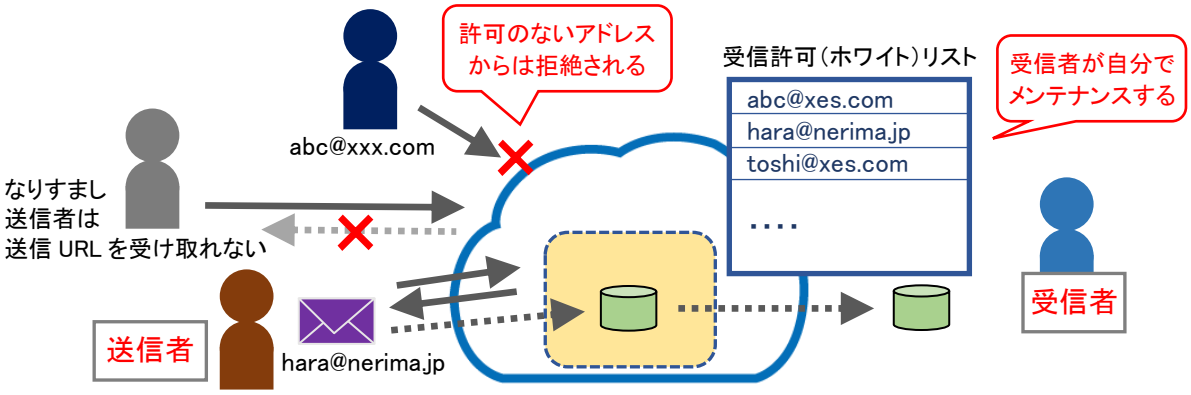
2. RSFファイル交換サービス - SafetyCarrier を使ったファイルの受け取り

ファイルを送る側は受け取る側へ依頼メールを送り、受け取る側は送信用の URL を用意し送る側へ返信、送る側は受け取った URL を使いファイルをアップロードします。



取引先からのファイル受け取りに限定するには、受信者が対象となる取引先のメールアドレスを予め登録します。登録されたメールアドレスのリストは、フィッシング防止の為の受信許可リスト（ホワイトリスト）の役割を果たします。RSFファイル交換サービスのオプション「受信許可のないファイル送信」を「**受信許可していない送信者からのファイルの受信はできない**」に変更することで、受信許可リストに掲載されていない送信者アドレスからのファイル送信が拒否される様になります。

RSFファイル交換サービスが持つ**なりすましが難しいという特性**と、この**受信許可リストの機能**を合わせて利用することで、**受信者が許可登録していないメールアドレスからのファイル送信を完全に受け取らない環境**が実現します。※



クラウド共有と違い、事前の認証情報の交換が不要で、ファイルの送信者（取引先）への過度な負担も必要ありません。

誰からのファイル送信を受け付けるのかをコントロールするのは、自社で運用するRSFファイル交換サービスの受信許可リストへの登録作業だけになります。

※ 当たり前のことですが、送信者のメールアドレスが第三者に乗っ取られていた場合、ファイルの送信を許してしまいます。