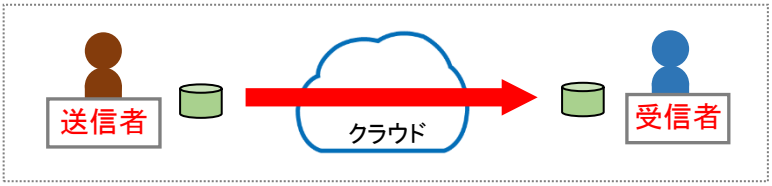
クラウドサービスを使ったファイル受信

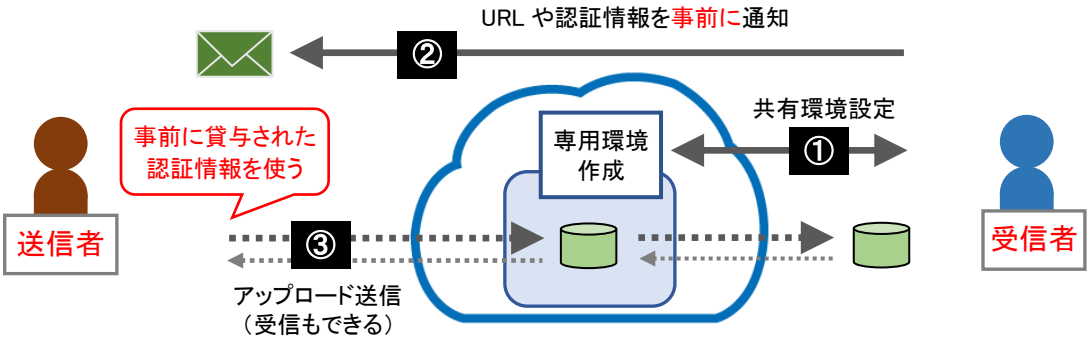
インターネットでファイルを送受信する場面に於いて、ファイルを受け取る側の用意するクラウドサービスを使った受け渡しの方法は、悪意の攻撃に対しても安全に利用することができます。

クラウドを通して、送信者から受信者へファイルを送る方法について紹介します。



1. SHARE 型

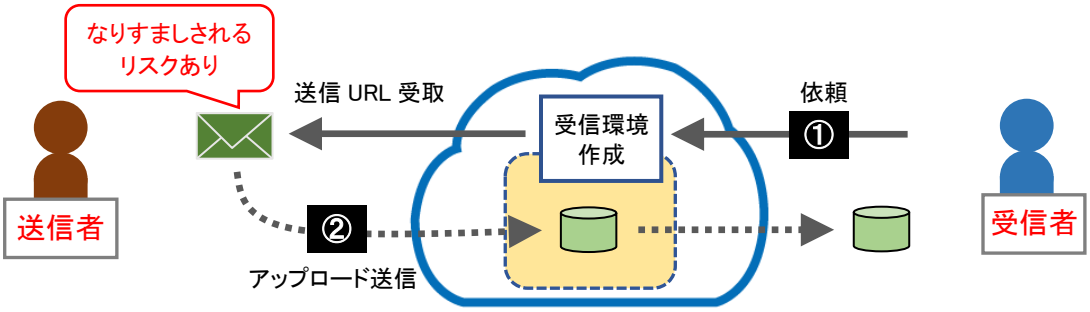
ファイルを受け取る側が送る側に、URL や認証情報を事前に貸与し、送る側は貸与された URL や認証情報を使いファイルをアップロードします



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 や認証情報を渡します(②)。
ファイルの送信者は、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)。共有領域を使って、受信者から送信者へファイルを受け渡しすることもできます。

2. PULL 型

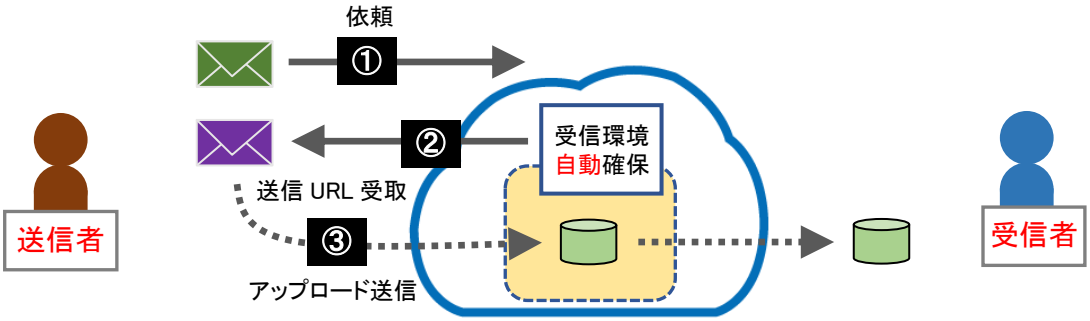
ファイルを受け取る側が送る側に URL などを含むリクエストを送り、送る側は受け取った URL を使いファイルをアップロードして送信します。



ファイルの受信者はクラウドサービスへファイル受信のための依頼を行います。クラウドサービスは送信者へ、ファイル送信のリクエスト通知を送ります(①)。
ファイル送信リクエストを受け取った送信者は、リクエスト通知に記載されている URL を使ってファイルをアップロードして、受信者へ送信します(②)。

3. PUSH 型　RSFファイル交換サービス - SafetyCarrier

ファイルを送る側は受け取る側へファイル送信のための依頼を送り、受け取る側は送信用の URL を用意し送り側へ返信し、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。



ファイルの送信者はクラウドサービスへファイル送信のための依頼を送信し(①)、ファイルの送信に使う URL を受け取ります(②)。
ファイルの送信者は、受け取った URL を使ってファイルをアップロードします(③)。
ファイルの受信者は、ファイルを受け取るまで操作の必要がありません。

4. 各方式の比較

	SHARE 型	PULL 型	PUSH 型
ファイル送受信の契機	どちらからも可能	受信者側	送信者側
URLや認証情報の受け取り	事前配布	送信時	送信時に URL のみ
送信者側の義務	認証情報の漏えい対策	ー	ー
送信者側のリスク 注 1	安全	騙される危険性あり	安全
受信者側のリスク	低い	低い	低い
受け渡し領域の管理	事前に設定が必要 アクセス権も設定	受信者が都度確保	システムが自動確保
受信ファイルの後処理	受信者が削除	受信者が削除	自動削除
特徴	取引先に限定したファイル交換	ファイルを受け取りたい時に要求を出す	ファイルを受け取れるアドレスを予め広報
注意事項 (受信者-システム提供側)	アクセス権設定などの共有領域の設定誤り	違う相手にリクエストを送る危険性あり	送信者を確認した受信を心掛ける
製品	多くのクラウドサービス	DropBox、Box など	SafetyCarrier

注1 クラウドサービスを模倣した WEB サービスと、なりすましメールによる攻撃はリスクになります。

※ クラウドサービスに係るリスクへの対策として、システムが対応することで守ることのできる(例えば、認証手段の強化、ウイルスやハッキングによる攻撃への対策)については、本書では取り上げていません。あくまでも各方式による特徴を比較したものです。