https://www.rsf.ne.jp/

RSFファイル交換サービス

SafetyCarrire　セイフティ・キャリアー

Receiver led Service for Files Exchange

最も手軽で安全に
誰からでもファイルを受け取れる

「なりすましメール」に強力に対抗する手段

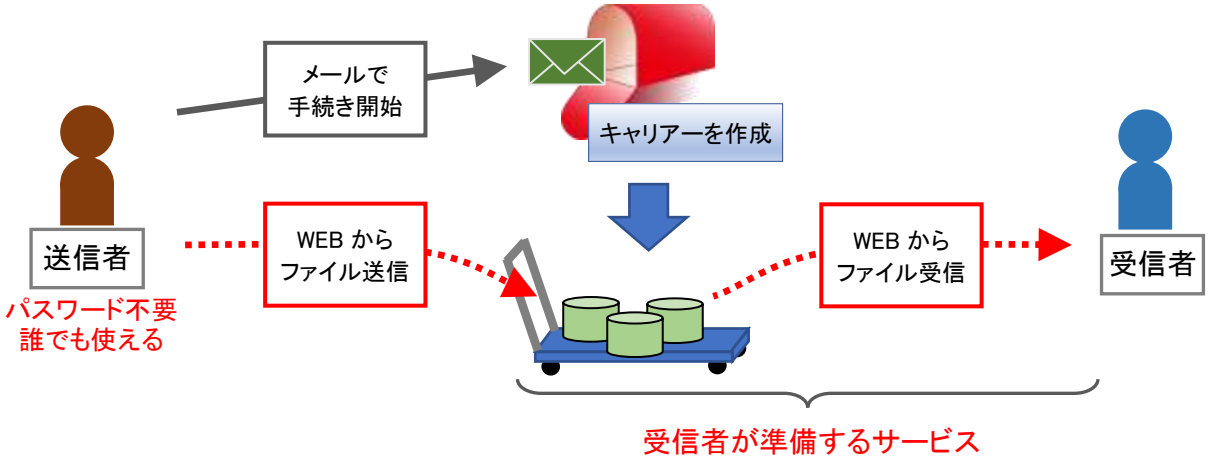
第 1.5 版　2022 年 3 月 6 日

株式会社 エクセス

－ 目次 －

1. 最も手軽で安全にファイルの受け渡しができるサービス

RSF ファイル交換サービスは、**ファイル受信者が主導**となってファイルの送受信手順を組み上げることにより、**認証情報の受け渡しの手順を踏むことなし**に、**誰からでも容易にファイルの受取ができる**サービスです。
また、**なりすましメールへの強力な防衛手段が備わっている**ことや、**誤送信対策**、**盗聴防止機能が備わっている**ことから、クラウドを使ったファイル共有方法に劣らない安全なサービスを提供します。



2. PPAP の代替として、RSF ファイル交換サービスが最適

- 誰とでも、認証情報を事前に交換せずに使える
- なりすましや、悪意の第三者からの攻撃に対抗する手段を備える
- 誤送信対策および盗聴防止機能を備える
- ファイルの送信手段は使い捨てのワンタイム方式、送り終えたら役目を終える
- 受信者が直接ファイルを取得するので、暗号化は不要、ウイルスチェックにも対応する
- 盗聴防止に利用するパスワードは、受信者自身が設定するので第三者に読み取られる心配がない

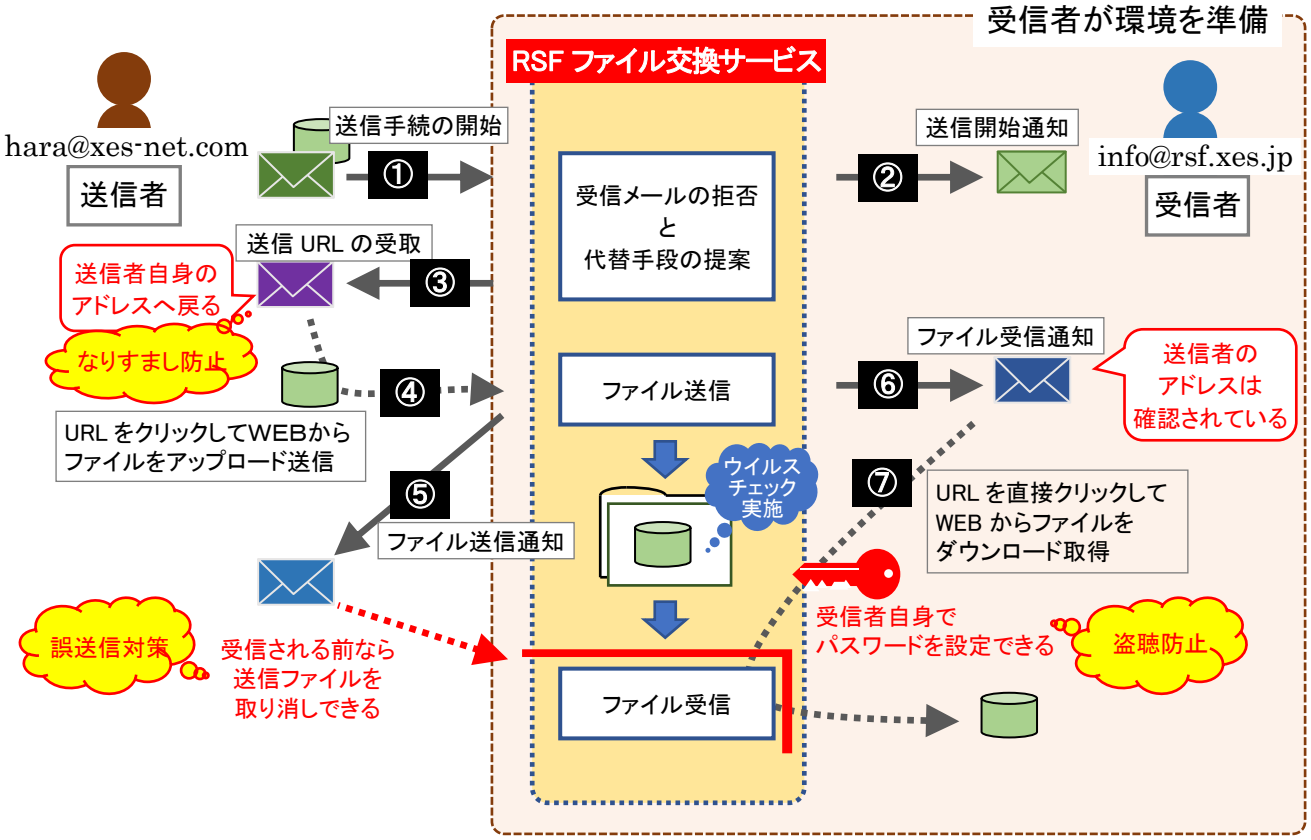
RSF ファイル交換サービスは、ファイルの共有ではなく、ファイルの送受信に特化したサービスです。送信されるファイルはクラウド上に貯め置かれて許可があればいつでもアクセスができるのではなく、送信者の手を離れたら受信者へ届けられる**一方通行**のサービスになります。

ファイルアクセス許可の設定ミスなどで情報漏えいが発生したりなど、人為的な事故の危惧されるクラウドストレージの共有とは違い、利用者によるファイルへのアクセス許可などを管理する必要もありません。

RSF ファイル交換サービスは、誰でも簡単に、そして安全に使えるファイル送受信環境を提供します。

3. ファイル送受信の詳細手順、メール･WEB のやり取り　受信モード

RSF ファイル交換サービスを使って、ファイルを受信する手順の詳細を以下に示します。
送信者ならびに受信者は、PC、スマートフォン、タブレットなどのメーラーと WEB ブラウザを使って利用できます。専用アプリは必要ありません。

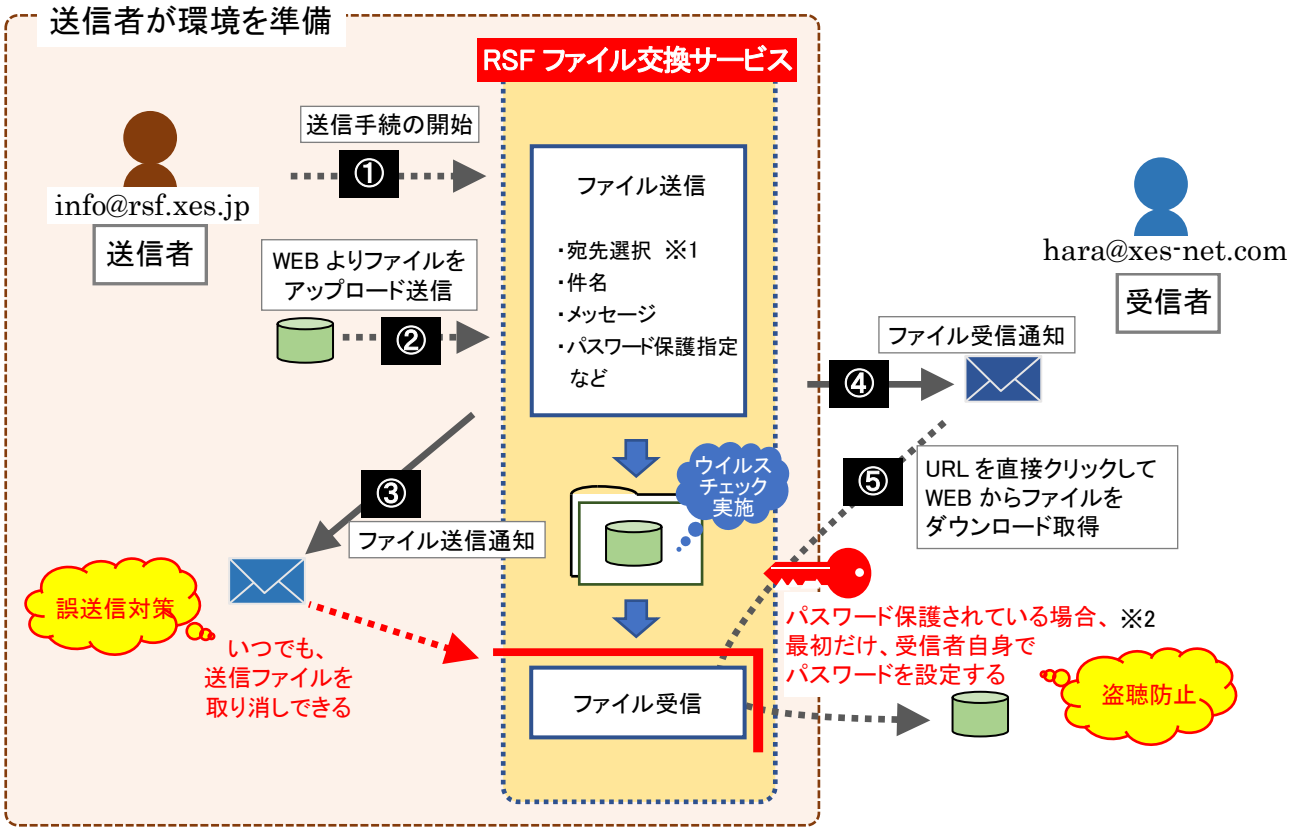


各処理の説明

	行動	目的	送信者の作業	受信者の作業
①	送信手続きの開始	ファイル送信キャリアーの発行依頼	(添付ファイル付き)メールの送信	ー
②	送信開始通知	送信が始まったことを知らせる	ー	メール受信のみ (何もする必要はない)
③	送 信　URL の受取	ファイル送信キャリアーの受取	メールを受信	ー
④	ファイルの送信	ファイル送信キャリアーへファイルをアップロードしてファイルを送信	メール記載 URL(ファイル送信キャリアー)をクリックしてファイルをアップロード	ー
⑤	ファイル送信通知	ファイルの送信が完了したことを知らせる	メール受信のみ (送信取り消し URL 受取)	ー
⑥	ファイル受信通知	ファイルが到着したことを知らせる	ー	メールを受信、ファイル送信者のアドレスなどを確認
⑦	ファイルの受信	ファイル受信キャリアーからファイルをダウンロードしてファイルを受信	ー	メール記載 URL(ファイル受信キャリアー)をクリックしてファイルをダウンロード(パスワード入力)

4. ファイル送受信の詳細手順、メール･WEB のやり取り　送信モード

RSF ファイル交換サービスを使って、ファイルを送信する手順の詳細を以下に示します。
送信するファイルをパスワード保護する・しないは、送信者によって指定されますが、パスワードは、ファイルの受信者自身が設定して運用します。（詳しくは、６．（２）を参照）



※1　宛先は、受信許可されているアドレスから選択します。受信履歴の無い宛先への送信をする場合は、予め受信許可リストへ登録できます。

※2　受信者パスワードは、受信者が自分自身で設定します。一度設定すると、以後同じ送信者からのファイル受信時のパスワードとなります。パスワードの変更、削除もいつでもできます。
パスワードの設定は、自身のメールアドレスで受け取る設定 URL から行うので、設定操作は必ず受信メールに履歴が残ります。第三者による不正アクセスに気が付く機会を逃しません。

各処理の説明

	行動	目的	送信者の作業	受信者の作業
①	送信手続きの開始	ファイル送信キャリアーの発行依頼	管理画面を認証して開く	ー
②	ファイル送信	ファイルをアップロード	WEB からファイルをアップロード	ー
③	ファイル送信通知	ファイルの送信が完了したことを知らせる	メール受信のみ（送信取り消し URL 受取）	ー
④	ファイル受信通知	ファイルが到着したことを知らせる	ー	メールを受信、ファイル送信者のアドレスなどを確認
⑤	ファイルの受信	ファイル受信キャリアーからファイルをダウンロードしてファイルを受信	ー	メール記載 URL（ファイル受信キャリアー）をクリックしてファイルをダウンロード（パスワード入力）

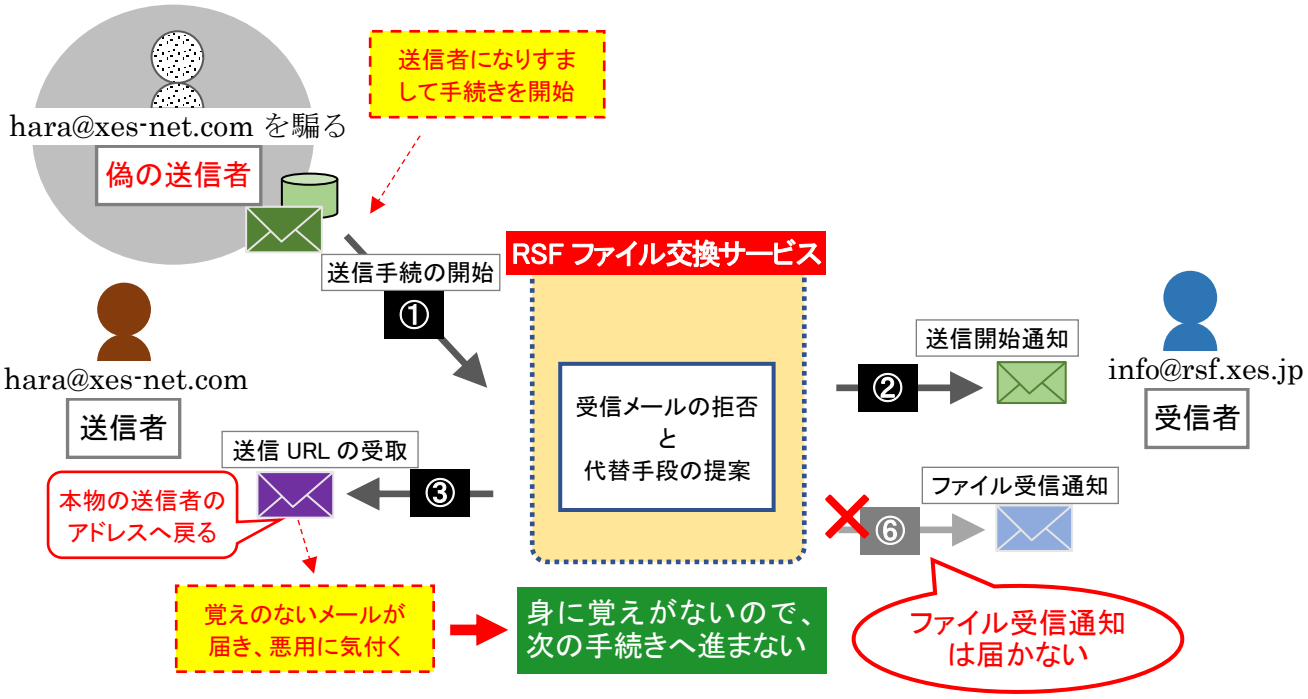
5. なりすましメールなどの介入ポイントと対策

５．（１）では、ファイルを送信する為には、送信者からの①「送信手続きの開始」に対して、RSF ファイル交換サービスから送られる③「送信 URL の受取」が必要になることを説明しています。
この一連の手続きが備わったことは、第三者によるなりすまし行為を防ぐことにつながります。

５．（２）では、だます目的の紛らわしいアドレスの送信者からの利用に対抗する手段として、受信を承認した送信者のホワイトリストで、人の目では判別し難い紛らわしいアドレスからの送信に対して、システムが警告を発する機能が備わっています。

５．（３）では、インターネットの公開ネットワーク上に RSF ファイル交換サービスを設置した際に、RSF ファイル交換サービスから受信者へ送られるメール通知が信頼性の担保できないネットワーク経路を使って送られた場合でも、偽装メールによるなりすましサイトへの誘導を暴く手段を提供しています。

（1）送信者のアドレスになりすました、偽の第三者によるファイル送信を阻止

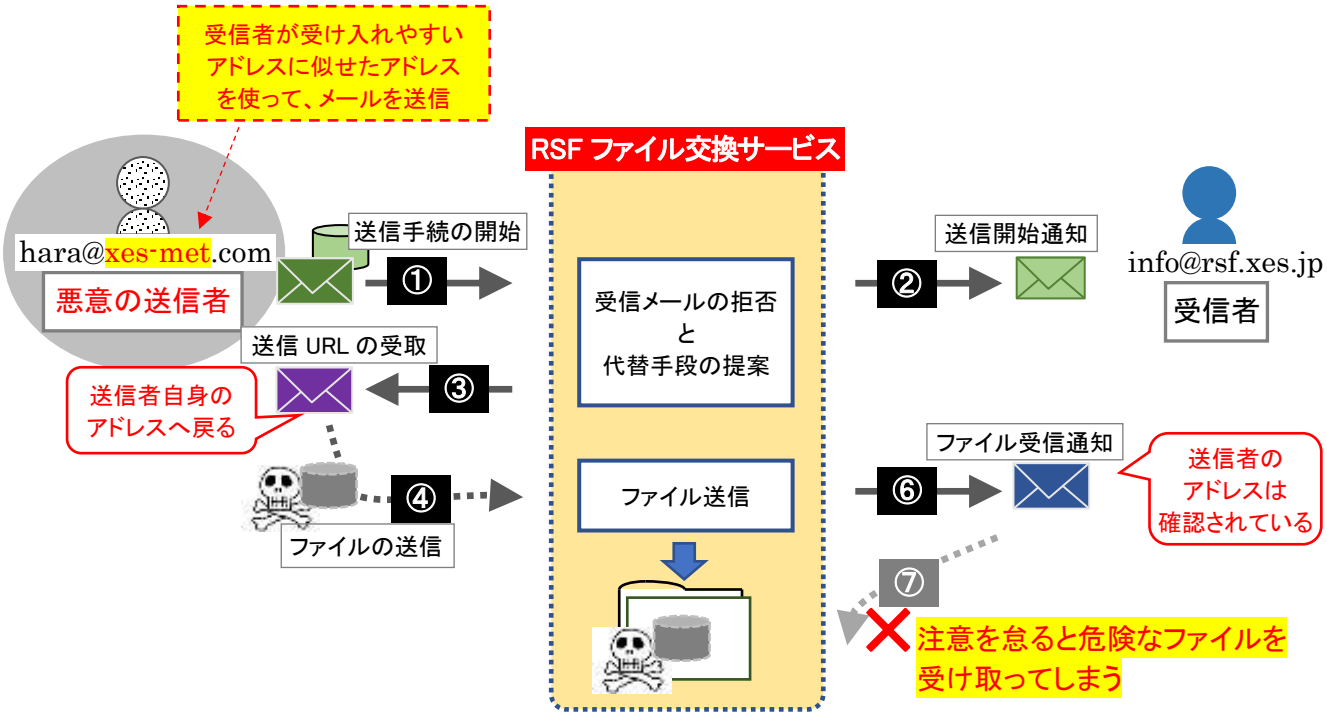


③の「送信 URL の受取」は、hara@xes-net.com へ届く為、偽の送信者の手に渡ることはありません。
偽の送信者は、送信 URL（ファイル送信キャリアー）を手に入れることができないので、ファイルを送信することはできません。

③の「送信 URL の受取」が届いた送信者は、自身のメールアドレスが第三者に悪用されたことを知り、関係者への注意喚起など適切な対応が図れます。

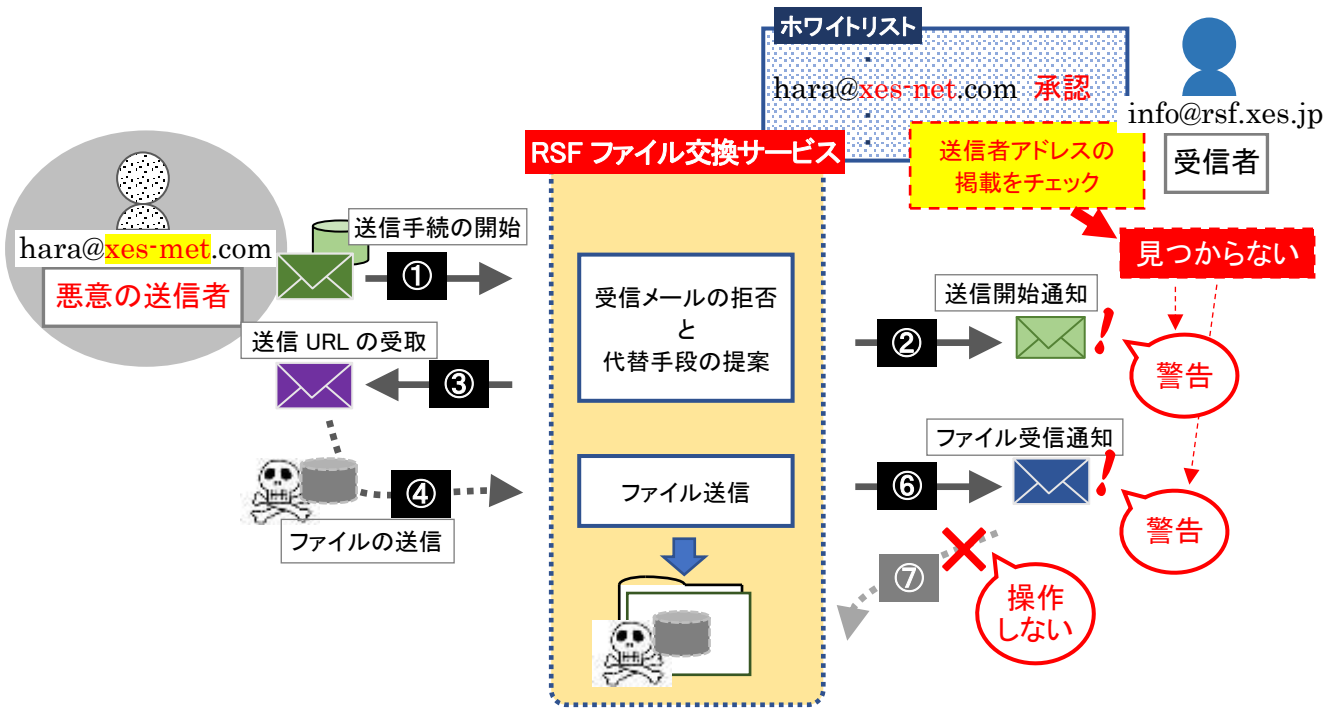
（2）だます目的の紛らわしいアドレスを使った、悪意の送信者からのファイル送信に警告

（ライセンス版機能）



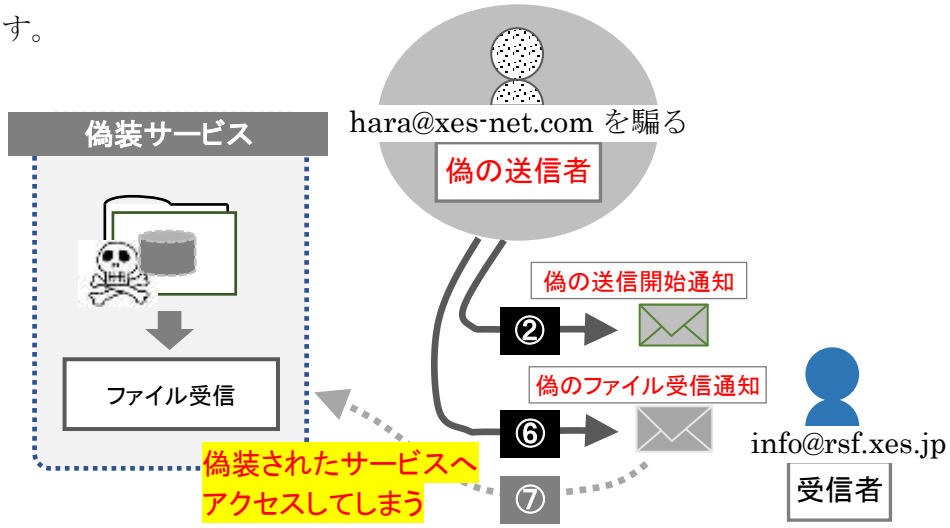
紛らわしいアドレスを使った悪意の送信者からのメールにだまされない為には、しっかりと送信者のアドレスを確認することが必要です。

ライセンス版では、正しくファイルを受け取れた送信者のアドレスを承認してホワイトリストを作成することができます。**ホワイトリストに掲載されていない（初めて届く）相手などからの通知に、警告を発する**ことができます。（承認操作は、ファイル受信時などに実施）



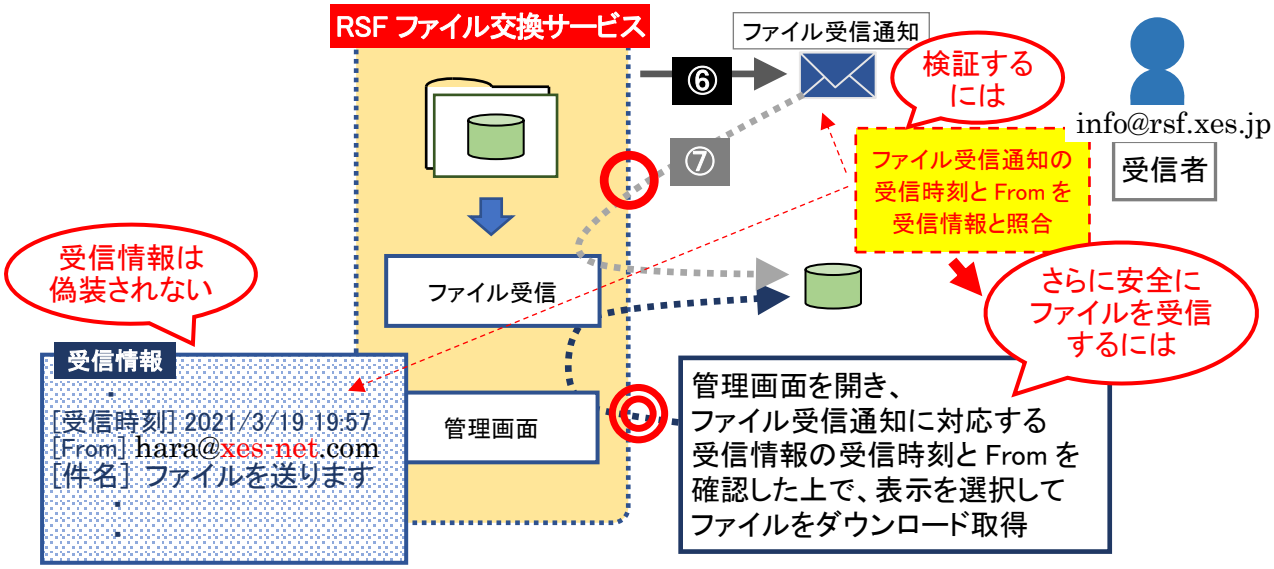
（3）通知メールのなりすましには、管理画面の確認を徹底することでだまされない

RSF ファイル交換サービスを自社ネットワーク内へ設置することで、システムより通知される各種メールの偽装を防ぐことができます。
しかし、クラウド上のサービスとして運用した場合には、社内メールサービスとの間に信頼の低いインターネット経路ができ、第三者による偽装などを
防ぐことが困難になります。



②「送信開始通知」と⑥「ファイル受信通知」の両方とも偽装された場合、メールに記載された URL を詳細に確認することで真贋を判断することができますが、だまされてしまう可能性がないとは言い切れません。

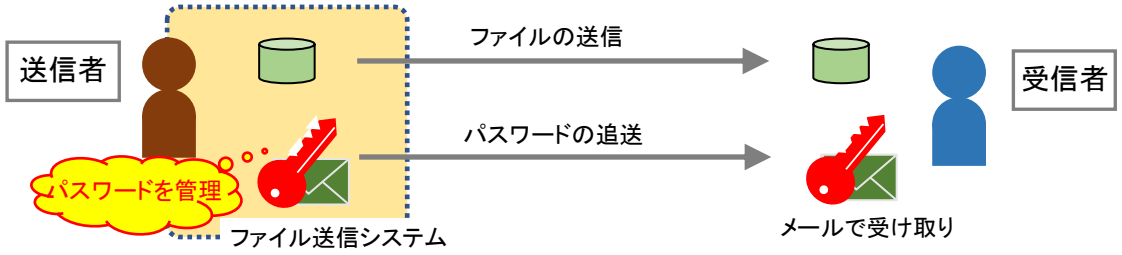
受信したメールが偽物でないことを確実に確認するには、「管理画面」の「受信情報」にメールで届いた通知に該当する情報が掲載されていることを確かめます。正しい手続きを経て届いたファイルの情報は、「受信情報」に掲載されます。受信時刻と From を確認します。
そして、ファイルのダウンロードは、⑥「ファイル受信通知」ではなく、「管理画面」の「受信情報」より選択して実施することで、より安全にファイルを取得することができます。



6. パスワードの受け渡し無しに盗聴を防ぐ

RSF ファイル交換サービスでは、ファイルを受け取る受信者自身が設定するパスワードを使って、第三者にファイルが盗み見られることを防ぎます。
PPAP やファイル送信サービスの様に、**ファイルの送信者から受信者へパスワードを通知することはありません。**

【PPAP やファイル送信サービス】



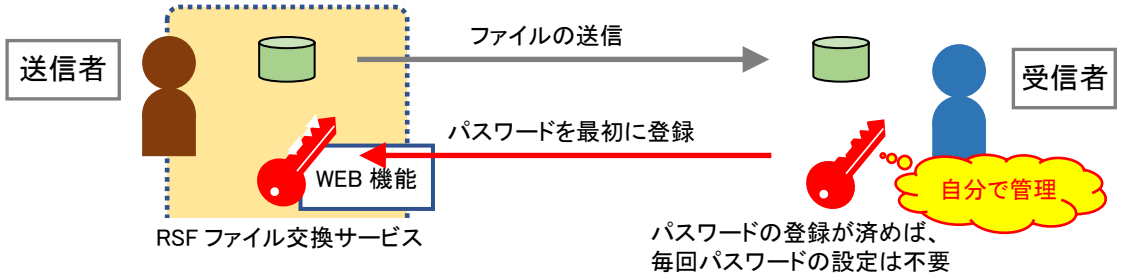
（1）受信モードで利用する場合のパスワード設定

3.（受信モード）で説明した環境で利用する場合は、RSF ファイル交換サービスの環境を用意する受信者が、管理画面のオプションからパスワードを登録し機能を有効にします。パスワードを有効にすると、ファイル受信通知に記載の URL を開く際にパスワードの入力が要求されます。
パスワードは受信者自身が設定し、他人に知られることなく自由に変更することができます。

（2）送信モードで利用する場合のパスワード設定

4.（送信モード）で説明した環境で利用する場合は、受信者が初めてファイルを受け取る時にパスワードを設定できます。
パスワードの設定はファイル受信ページから操作します。操作を開始すると、受信者自身のメールアドレスへ設定リクエストが通知されます。記載の URL からパスワードを入力できる WEB ページを開き、ここから設定します。**設定できるのは受信者自身だけ**になります。

【RSF ファイル交換サービス】



・ パスワードはファイルの受信者自身が設定し、いつでも変更・削除できる

パスワードの設定を実施するオペレーションは、ファイルを受信する画面からではなく、受信者自身のメールアドレス宛に送信される「受信者パスワードの設定」メールに記載されている URL から起動するホームページを通じてのみ、変更ができます。パスワードの削除も同様です。
これにより、**パスワードの変更操作が必ず自身のメールアドレスに履歴として残る**様になります。
仮にメールを覗き見ている第三者によるパスワードの変更操作が発生した場合でも、不正を発見する機会を逃すことはありません。

一度パスワードを設定すると、該当の送信者から届くファイルを受信する際のパスワード入力全てに有効なパスワードとなります。
また、パスワードの変更や削除は、前述のメール操作を通じていつでも行うことができます。

・ パスワード保護機能は、ファイルの送信時に選択する

送信されるファイルの受信者パスワード保護は、**ファイルを送信する時に毎回指定**できます。
「利用しない」、「受信者が利用する・しないを選択できる」、「パスワードの利用を求める（パスワード保護する）」から、送信するファイルの機密レベルに応じて選択できます。

・「受信者が利用する・しないを選択できる」を選択した場合

ファイルの受信者がパスワードを登録していない状態では、パスワードを登録して受信することも、パスワードを登録しないで受信することも、どちらも選択できます。
既にパスワードを登録してある場合は、パスワードの入力が必ず求められます。

・「パスワードの利用を求める（パスワード保護する）」を選択した場合

ファイルの受信者は、パスワードを登録していない状態では、パスワードの登録が要求されます。
既にパスワードを登録してある場合は、パスワードの入力が求められ、登録してあるパスワードを変更または削除する操作も選択することができますが、**ファイルを受信する為には必ずパスワードの入力が必要**になります。
もしも、パスワードを忘れた場合は、変更操作からパスワードを設定し直すことで対応ができます。

パスワードの安全性

RSF ファイル交換サービスは、PBKDF2 方式を使った安全なパスワード運用を実装しています。
同じ値のパスワードを利用者が設定した場合でも、システム上で管理するデータは異なったものとなり、また、管理するデータから元のパスワードを求めることも困難な仕様となっています。

7. PPAP、クラウドストレージ共有、RSF ファイル交換サービスの比較

（1）サービスの特徴

	特徴	PPAP（注 1）	クラウドストレージ共有（注 2）	RSF ファイル交換サービス
1	サービスの目的	ファイルを送受信する為の手段	本来の目的はインターネット上のファイル共有	ファイルを送受信する為のサービス
2	利用コスト	無料から始められ、無料で続けられる	無料サービスもあるが、目的を達成するには有料サービスが必要	無料サービスもあるが、よりセキュリティを重視するのであれば、有料サービスが必要

注 1　想定している PPAP は、ZIP 暗号化したファイルと復号パスワードを同じメールアドレス宛に 2 回に分けて送信する、一般的な利用方法を想定している
注 2　PPAP の代替案として、クラウドストレージなどを使ったファイル共有による、ファイルの受け渡しを想定している

（2）課題・問題点・解決状況

以下、赤 ： 問題のある点、黄 ： 問題となる可能性がある点、緑 ： 優れている点

	課題・問題点		PPAP（注 1）	クラウドストレージ共有（注 2）	RSF ファイル交換サービス
1	盗聴	第三者に受信される	パスワードを同一経路で送信しているので防げない	閲覧パスワードで保護	受信パスワードで保護
2		送信経路で覗き見られる	パスワードを同じ経路で送っているので覗き見られる可能性あり	クライアントからの直接アクセスなので問題なし	クライアントからの直接アクセスなので問題なし
3	誤送信	送信を取り消しする	パスワードメールの送信をしないことで可能	システムが用意している範囲で対応が可能（製品による）	ファイルが受信される前であれば取り消しが可能
4		間違った相手に届いてしまったら	対応不可	対応不可	対応不可
5	安全性	パスワードの安全性	脆弱なパスワード、総当たり攻撃ツールで容易に復号が可能	強いパスワードに対応（製品による）	強いパスワードに対応
6		ウイルス・マルウエアへの対策	ウイルススキャンができない	ウイルススキャンが可能（製品による）	ウイルススキャンに対応
7	認証の為の事前準備	利用主体から送受信相手へ渡す情報	なし	安全な手段で、共有の為の認証情報の事前配布が必要	なし

続く

続き

	課題・問題点		PPAP（注 1）	クラウドストレージ共有（注 2）	RSF ファイル交換サービス
8	作業量・手順	送信の手順	ZIP 暗号化ファイルとパスワードの 2 通のメール送信が必要	パスワード認証してアップロード操作	メールを送った後に返信メールからアップロード操作
9		受信の手順	受信した 2 通のメールを確認し ZIP ファイルを復号してファイルを取得	パスワード認証してダウンロード操作	受信通知からダウンロード操作（受信パスワードの利用も可）
10	同報送信	複数の相手先への一括送信	できる（Cc、Bcc 送信にも対応） 但し、パスワードは全て同じ	対応するシステムであれば可能だが、事前設定などが必要	できる（Cc、Bcc 送信にも対応） 全ての受信者へ違う URL が届く
11	受信側が主体となって利用した場合	誰からでも受信できるか	誰からでも受け取れる	事前登録した相手からだけしか受け取れない	誰からでも受け取れる
12		送信者の管理すべき認証情報など	なし（暗号化パスワードは一時管理）	預かった認証情報	なし（受け取った URL はワンタイム）
13		受信者の管理すべき認証情報など	なし（複合パスワードは一時管理）	各送信者へ渡す認証情報と自身の認証情報、共有の情報など多数	管理機能のパスワードと、受信パスワード（1 種類、任意利用）のみ
14		システム管理者の作業量	少ない	多い（アクセス権限、共有、フォルダー管理など）	少ない
15	送信側が主体となって利用した場合	誰へでも送信できるか	誰へでも送れる	事前登録した相手だけ 認証なしで送れるのであれば可能だが、セキュリティ上のリスクが伴う	受信を承認している送信者宛に送れる ただし、なりすまし対策機能などは働かない
16		送信者の管理すべき認証情報など	なし（但し専用システムなどを使った場合は認証情報などあり）	各受信者へ渡す認証情報と自身の認証情報、共有の情報など多数	管理機能のパスワードと、受信パスワード（1 種類）のみ
17		受信者の管理すべき認証情報など	なし	預かった認証情報	なし
18		システム管理者の作業量	少ない	多い（アクセス権限、共有、フォルダー管理など）	少ない

続く

続き

	課題・問題点		PPAP（注 1）	クラウドストレージ共有（注 2）	RSF ファイル交換サービス
19	なりすまし対策	正規の送信者アドレスを騙った送信	対策不可	認証が前提であれば送信されない	正規のアドレスからは送信されない
20		紛らわしいアドレスからの送信	騙される可能性あり	認証が前提であれば送信されない	送信者の承認機能で警告が発せられる
21		偽サイトなどへの誘引（送信側）	ー	偽サイトで認証情報を盗まれる可能性がある	送信者に盗まれる認証情報などはない
22		偽サイトなどへの誘引（受信側）	ー	偽サイトで認証情報を盗まれる可能性がある	偽サイトで認証情報を盗まれる可能性がある
23	最悪のシナリオ	第三者に端末が乗っ取られていた場合	対策不可	対策不可	対策不可

（3）その他

	弱点・利点	PPAP（注 1）	クラウドストレージ共有（注 2）	RSF ファイル交換サービス
1	弱点	盗聴防止できない ウイルスチェックできない 送信・受信に手間がかかる なりすましメールに騙される	送受信相手毎に、認証情報の事前交換が必要で、認証情報の管理は提供先に委ねられる アクセス権や共有領域の設定など事前に正しく設定する情報が多く、誤った設定をした場合、致命的な問題につながるおそれがある 偽サイトを通じて認証情報を奪取される可能性がある	サービスの利用者が送信に使用する場合、なりすまし対策機能などが働かない為、受信者側にURL の受け渡しに関わるセキュリティ上のリスクが伴い、一般的なファイル送信サービスと同等のセキュリティレベルとなる 但し、承認済みの送信者へしか送れないことで、悪質な送信に利用されることを抑止している
2	利点	手軽で、誰でも使える	信頼関係のある取引先とのファイル交換に向いている	誰からでもファイルを受け取れて、管理する認証情報の数が少ない

8. 利用方法と導入の形態

（1）RSF ファイル交換サービスの提供するメールアドレスで利用する

⇒　① メール ID 単位

ホームページよりアドレスを取得してサービスを利用する

（2）専用ドメインのメールアドレスで利用する

A. クラウド

⇒　② 専用ドメイン型

SaaS サービスで専用システムを利用する

⇒　③ システム提供型

PaaS サービス上に専用システムを構築して利用する

B. オンプレミス

⇒　④ システム提供型

ハードウエアシステム上に専用システムを構築して利用する

9. サービス･機能と導入の形態

サービス・機能と、導入の形態との関係

サービス･機能		①メール ID 単位		②専用ドメイン型	③④システム提供型
		無料版	ライセンス版		
ファイル送信キャリアーの作成契機	全てのメール受信時	○	○	○	○
	ファイルが添付されたメールの受信時だけ	×	○	○	○
	件名が特定文字列ではじまるメールの受信時	×	○	○	○
なりすまし防止	送信者アドレスの実在確認	○	○	○	○
	未承認送信者の警告	×	○	○	○
	未承認送信者の受信拒否	×	○	○	○
盗聴防止	ファイル受信パスワード	×	○	○	○
誤送信対策	送信ファイルの取り消し	×	○	○	○
同報送信	複数宛先（Cc、Bcc 含め）	×	○	○	○
管理機能	受信一覧、選択受信	○	○	○	○
	受信許可（アドレス承認）	×	○	○	○
	キャリアー作成契機の変更	×	×	○	○
	転送先アドレスの変更	×	△注1	○	○
承認済み送信者宛のファイル送信		×	○	○	○

注 1　登録後のライセンス版機能を無料で利用できる 30 日間は利用できない

10.　サービスの仕様

サービスの仕様、機能の制限値

機能	①メール ID 単位		②専用ドメイン型	③④システム提供型 注 2
	無料版	ライセンス版		
同時に作成できるファイル送信キャリアー数	1	制限なし	制限なし	制限なし
送信できるファイルのサイズ	50MB	50MB	50MB	50MB
一回に送信できるファイルの数	5 個	5 個	5 個	5 個
一回に送信できるファイルの合計サイズ	100MB	100MB	100MB	100MB
受信ファイルの保存期間	7 日間	30 日間	30 日間	30 日間
承認（受信許可）できるアドレスの数	ー	制限なし	制限なし	制限なし
同報送信できる送信先の数	ー	制限なし	制限なし	制限なし

注 2　③④システム提供型は、カスタマイズにより仕様変更が可能です

https://www.rsf.ne.jp/

株式会社 エクセス
https://www.xes.ne.jp
〒179-0085 東京都練馬区早宮 1-18-15
mailto:info@xes.ne.jp
TEL 03-3991-5716　FAX 03-3991-3896
XES-NET
COMMUNITY INTERNET SERVICE

2022/3/6 版