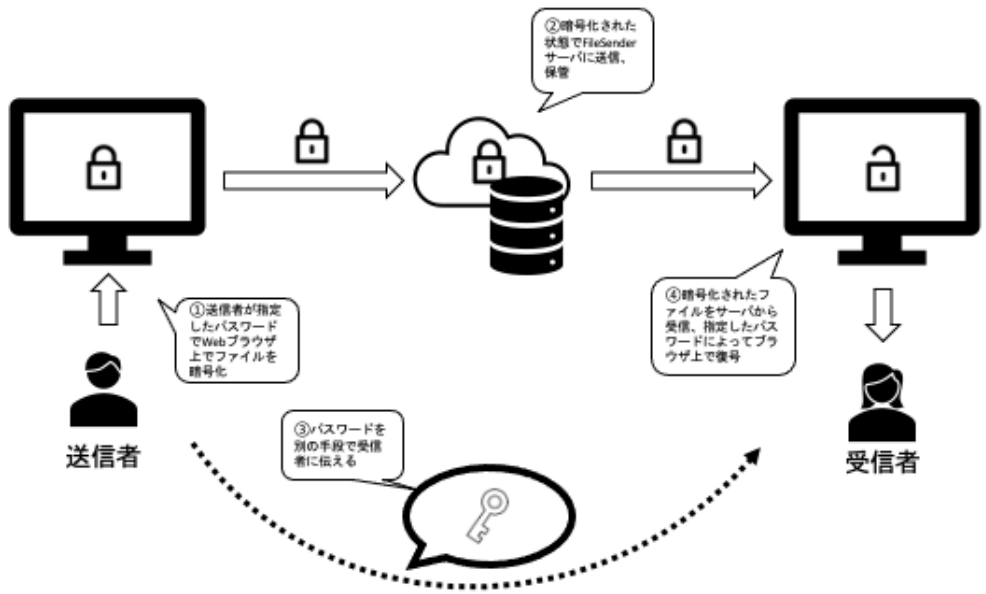
ファイル暗号化

FileSenderでは、ファイルを送信時にエンドツーエンドで暗号化、すなわちファイルの送信時に利用者のブラウザでファイルを暗号化し、受信時にブラウザで復号することができます。FileSenderとの間の通信経路およびFileSenderのサーバ内で暗号化された状態でが扱われるため、秘匿性を高めることができます。

暗号化のためのパスワードは送信する利用者のブラウザで暗号化時にのみ利用されますので、FileSenderのサーバ管理者ですらファイルの内容を見ることはできません。また、パスワードはFIleSenderでは管理、保存しませんので、送信する利用者が何らかの方法で受信する利用者に伝える必要があります。FileSenderでファイル送信時の「メッセージ」にパスワードを書き込むことは、そのメッセージが電子メールで平文のまま送られ、またFileSenderのデータベースに記録されることから、強くお勧めしません（暗号化したファイルとパスワードが一緒に取り扱われるため、暗号化している意味が薄れてしまいます）。

暗号化／復号は利用者のブラウザで行われるため、ブラウザの性能および利用するデバイスの性能に影響をおよぼします。大きなファイルを取り扱う場合、相応の時間およびデバイスのリソース（CPU、メモリ）を使用しますので、ご注意ください。

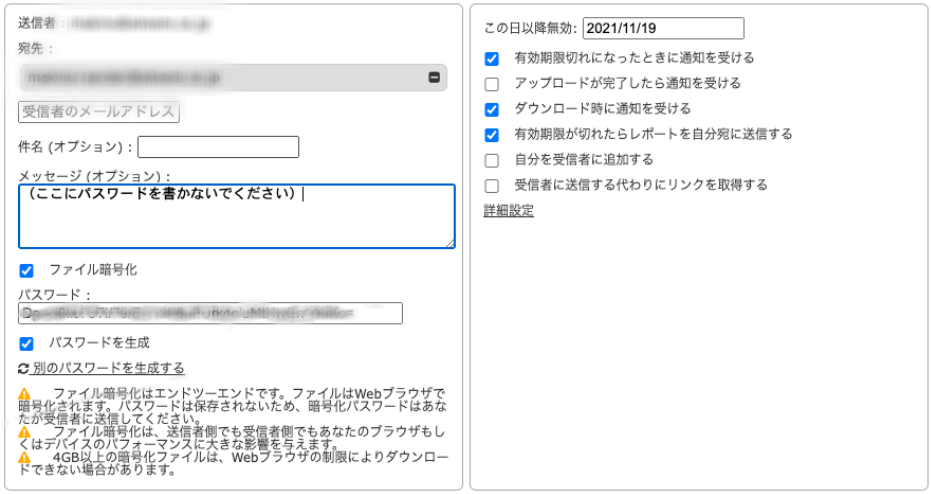
ブラウザでの暗号化／復号は、Webの標準として定義された Web Cryptography API (W3C Recommendation 26 January 2017) に基づいてブラウザが実装している暗号化／復号の仕組みを利用しています。暗号化のアルゴリズムは、"AES-GCM"です。



ファイルを暗号化して送信

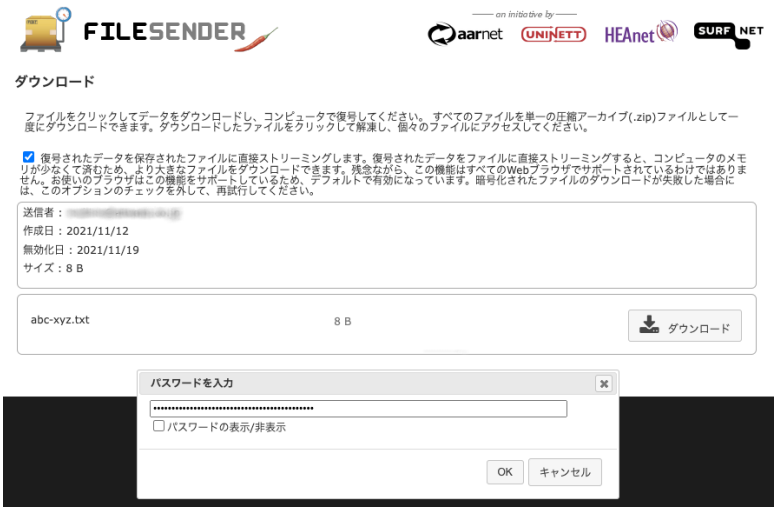
「アップロード」画面でファイルを送信時に「ファイル暗号化」をクリック（チェック）し、任意の暗号化するパスワードを入力してください。
「パスワードを生成」をクリック（チェック）すればランダムな文字列（アルファベット小文字／大文字、数字、記号を混ぜた44文字）のその場限りで有効なパスワードを生成します。必ずファイルを送信する前に生成されたパスワードを控えてください。

「送信」ボタンをクリックするとパスワードを使ってファイルを暗号化した後、アップロードします。パスワードは二度と見ることができなくなりますので、注意してください。



暗号化されたファイルの受信

暗号化されたファイルの場合、「ダウンロード」画面で「ダウンロード」ボタンをクリックするとそのパスワードの入力が求められます。ファイル送信者が設定したパスワードを入力することでファイルがダウンロードできます。パスワードが誤っているとダウンロードできません（ブラウザの警告が表示されダウンロードが始まりません。暗号化されたファイルをダウンロードすることもできません）。



パスワードを誤って入力した場合の表示

