2021.11.23

Joomla におけるテキストフィルタについて

1．所在

グローバル設定　＞　テキストフィルタ

2．機能

・下記のテキキストフィルタ機能は、Joomla サイトのセキュリティ保持の観点から大変重要な機能で、特にコンテント作成・投稿時にその効果を発揮します。

・この機能は、特にサイト設計者が知らなければならない機能です。つまり、一般の外部者からのサイトへのコンテント投稿を設計する場合は、そのフォーム設計だけでなく、同時にこのテキストフィルターを相応しい機能に割り当てる必要があります。
特に高い役割（Editor,Publisher など）を持たせる外部者には、注意しておく必要があります。

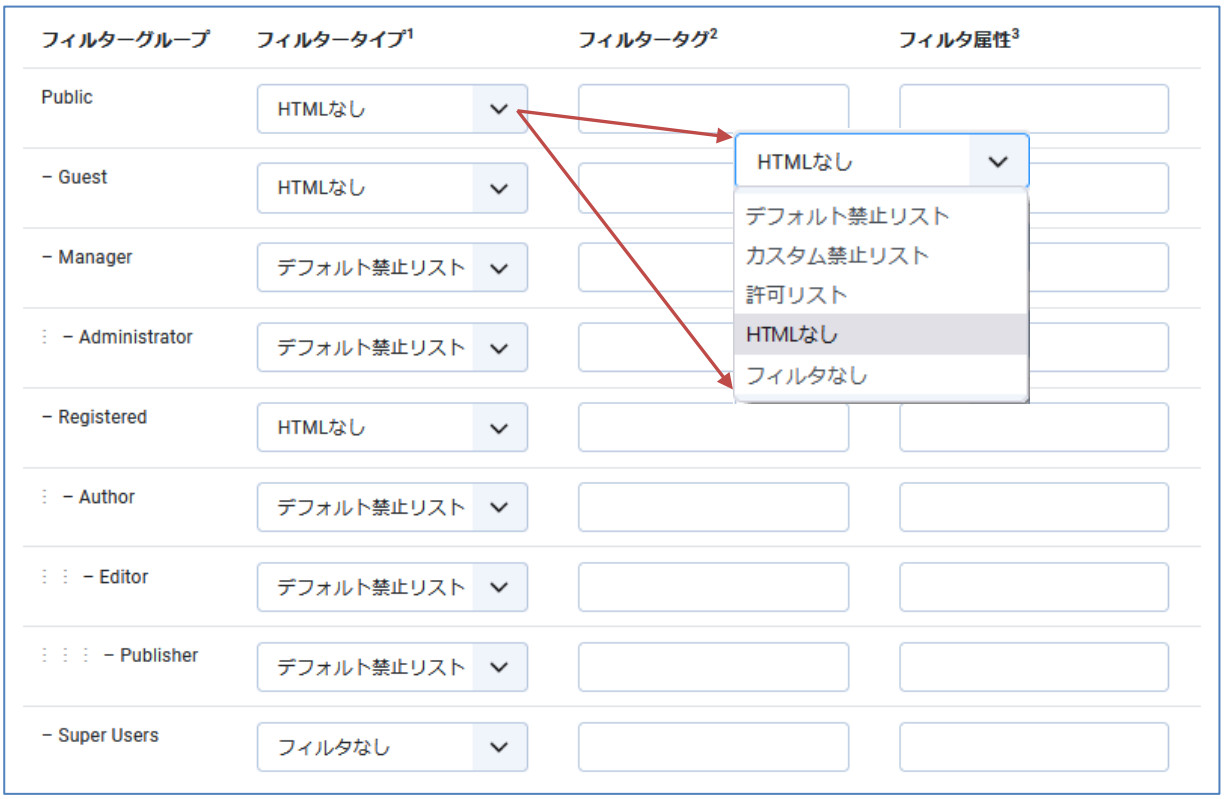
3．テキストフィルタの役割

これらのテキストフィルタ設定は選択されたグループ内のユーザに対し投稿されたすべてのテキストエディタの項目に適用されます。

これらのフィルタリングオプションは、コンテンツ提供者の送信する HTML を制御するものです。

サイトのニーズ・必要性に合わせて、厳格にしたり、緩和したりすることができます。フィルタリングはオプトイン（受領者主体。下記注）で、標準設定は一般的にウェブサイトの攻撃に関連付けされたマークアップに対しての保護に有効なものが提供されています。

4．テキストフィルタ設定画面（初期設定状態）



（注）「オプトイン」と「オプトアウト」

「オプトイン」とは、参加するとか加入するという意味。「オプトアウト」は、不参加とか脱退するという意味。

この二つの仕組みで一番重要なのは、**「主導権がどちらにあるか」**ということです。**オプトアウト**方式ではメールの送信者側に主導権があり、**オプトイン**ではメールの受信者側に主導権があるということに注目してください。

オプトアウト方式では、受信者が出来ることは受信拒否に限定されますが、オプトイン方式では受信者がメールを受信するにあたり事前にその趣旨や内容を吟味できることになります。極端な話、受信者が「メールを送っていいですよ」（受信の許可）と言わなければメールが届くことはありません。

5. フィルタータイプ

禁止リストは、リストされているものを除き、すべてのタグと属性を許可します。＜太字は J4 で追加＞

- デフォルトの禁止リストには次のタグが含まれます：

  「applet」,「body」,「bgsound」,「base」,「basefont」,**「canvas」**,「embed」,「frame」,「frameset」,「head」,「html」,「id」,「iframe」,「ilayer」,「layer」,「link」,「meta」,「name」,「object」,「script」,「style」,「title」,「xml」

- デフォルトの禁止リストの属性は次のとおりです。

  「action」,「background」,「codebase」,「dynsrc」,「lowsrc」,**「formaction」**

- 更にタグと属性をタグのフィルターに追加して、追加のタグと属性を禁止できます。各タグまたは属性名はコンマで区切ります。
- カスタム禁止リストを使用すると、デフォルトの禁止リストを上書きできます。タグと属性のフィルタ欄に禁止するタグと属性を追加します。

- 許可リストはタグと属性のフィルタ欄に記載のタグのみを許可します。

- HTML なしは、保存時にすべての HTML タグをコンテンツから削除します。**（最大の制限）**

（注）これらの設定は、使用しているエディターに関係なく機能することに注意してください。

WYSIWYG エディターを使用している場合でも、フィルター設定により、データベースに情報を保存する前に、追加のタグと属性が削除される場合があります。

6. フィルタータグ

- 追加のタグをリストし、各タグ名をスペース又はコンマで区切ります。

  例　p,div,span

7. フィルタ属性

- 追加の属性をリストし、各属性をスペース又はコンマで区切ります。

  例　class,title,id

8. 試行テスト

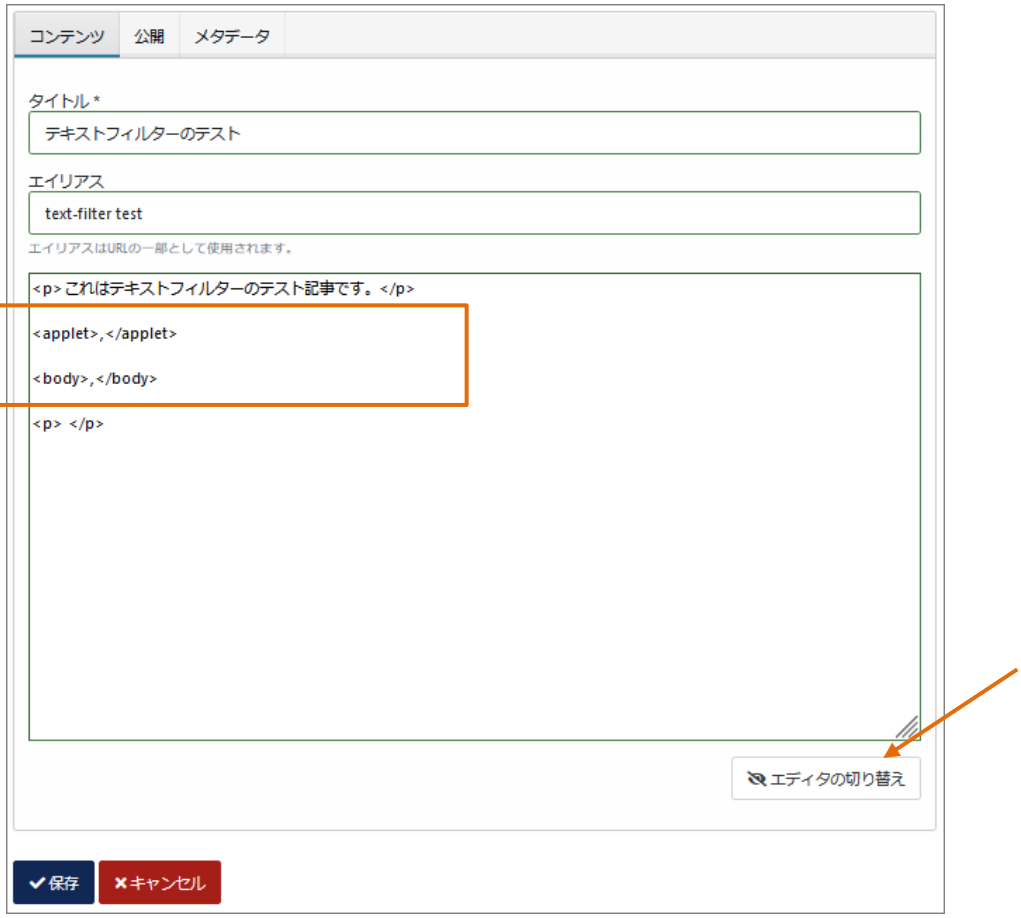
1）TinyMCE エディターを使用　（投稿者は、Register 設定）

確認：　グローバル設定　＞　パーミッション

←「未許可」から「許可」に変更
（デフォルトは未許可）

2）フロントエンド　＞　ログイン　＞　投稿画面

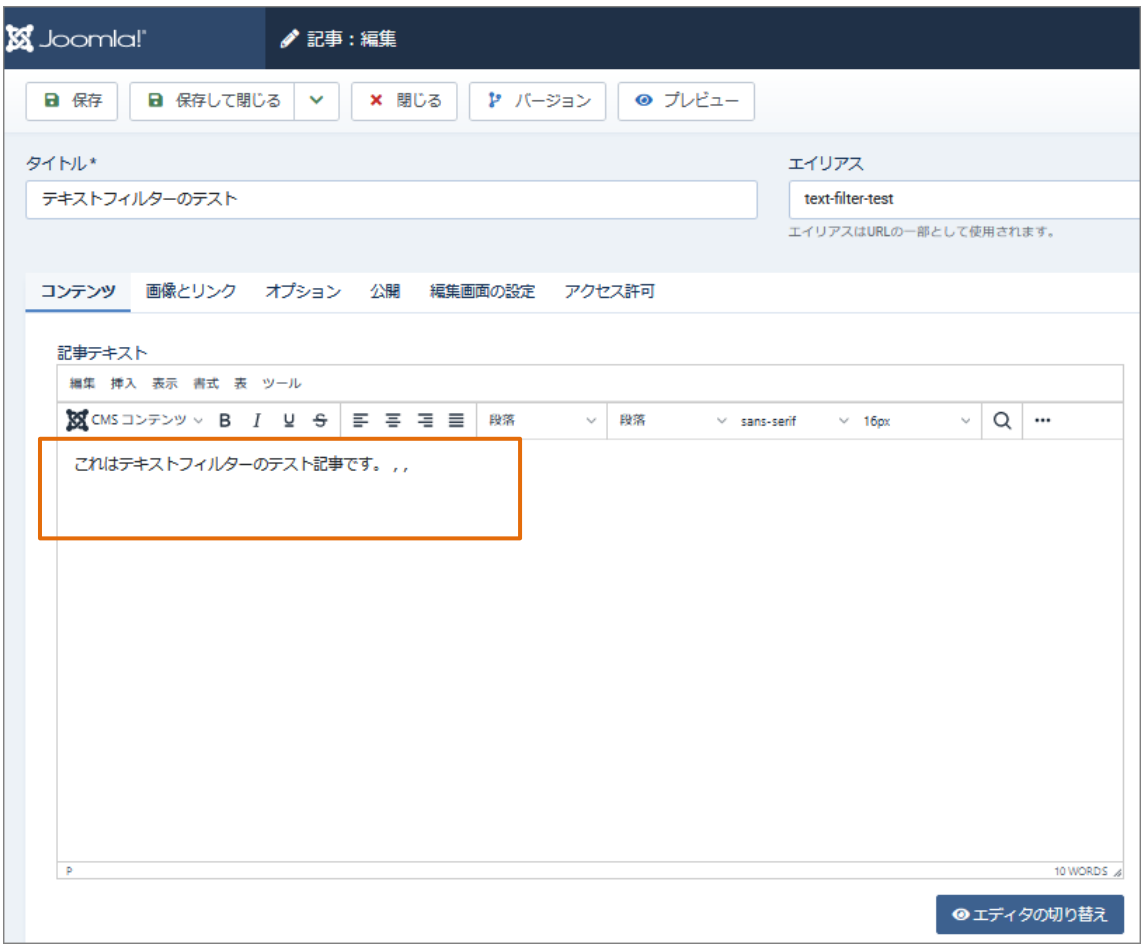
- 右下の「エディタの切り替え」ボタンをクリック（html 形式入力に）
- 禁止ワード「applet」と「body」を記述



3）投稿　正常に完了

4）バックエンド　記事管理ページ

記事をクリックし、開ける。　**禁止ワードが削除**されている。



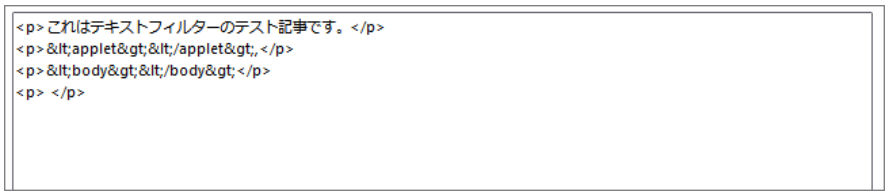
エディターを切り替え、html 画面。同様に禁止ワードは削除されている。

2）結果と対策

- 上記のように、グローバル設定　＞　テキストフィルターのレベルを適切に、ユーザ毎に適切に設定する。

- 参考）エディタの　「テキスト編集画面」を使い、禁止ワードを定義する。

これを「エディターの切り替え」ボタンをクリックし見ると、



禁止ワードが変更されており、投稿しても無害である。従って、「エディタの切り替え」ボタンを公開しなければ、強い制限がかけられる。

参考）http://joomt.blogspot.com/2013/01/configure-text-filter-settings-in.html

以上