主に日本製のユーザスクリプトのリンク集として機能しており、国内のユーザスクリプトが沢山掲載されています。Greasemonkey以外の情報もとても多いので、まだ見たことがなければ是非この機会にチェックしておきましょう。

二点目は「Greasemonkeyとは？」でも紹介した「userscripts.org」です。なんと言っても6000件以上も登録されていると言うのは凄まじいものがあります。登録されているユーザスクリプトはタグで分類されているので、登録数にも関わらず目的のものが探しやすくなっています。海外のサイトなので基本は英語ですし、登録されているユーザスクリプトも海外のサイト向けの物が多いのが難点です。

三点目の「はてなグリースモンキー」はまとめとは少し違いますが、「はてな」内で使うことを前提としたスクリプト集となっています。はてなを使っている場合はどれも便利なスクリプトなので、こちらも活用しましょう。

また、本書後半の「SAMPLES」では筆者のお薦めする厳選ユーザスクリプトも紹介しています。便利なスクリプトを沢山集めましたので、是非参考にして下さい。

1-2-9 配布スクリプトを使う場合の注意点

基本的にはどんなソフトウェアでもそうなのですが、「得体の知れないスクリプトは絶対にインストールをしない」と言うことは常に頭に置いておきましょう。

Greasemonkeyのユーザスクリプトはとても手軽にインストールできるので忘れてしまいがちなのですが、ソフトウェアのインストールには常に危険が伴います。もちろんGreasemonkeyも例外ではありません。最近ではウィルス対策ソフトも進化してきているので、こういう心配をすることは少なくなってきましたが、Greasemonkeyのユーザスクリプトに対しては、ウィルスやスパイウェアの対策ソフトはまったく役に立ちません。ユーザスクリプトに危険があるかどうかは自分自身で判断するしかないのです。

一体どんな危険があるのでしょうか？

Cookieが盗まれるなんてことは当然で、キーボードの入力内容からページの閲覧履歴などの個人情報にあたるものまで、かなりの情報を盗むことが可能です。恐ろしいことに、閲覧していないサイトの情報までも勝手に盗むことができてしまいます。

これらの危険を防ぐにはどうしたら良いのでしょうか？

ユーザスクリプトの内容をすべて読んで理解することができればもちろんこんな心配とは無縁です。ですが、それもなかなか難しいことだと思います。最低限、作者が信頼できるか、信頼できる人が使っているか、が押さえられなければインストールは控えた方が良いかもしれません。

どうしても得体の知れないスクリプトをインストールをしたいけど、ユーザスクリプトは読めない！と言う方は、最低でも次に示すキーワードがスクリプト中に含まれていないかはチェックしておきましょう。

① **document.cookie**
② **GM_xmlhttpRequest**
③ **無関係なページのURL**
④ **難読化されていないか**

「①document.cookie」は閲覧中のウェブサイトのCookie情報を取得するのに使います。これが含まれていた場合はCookieを操作するスクリプトだと言うことです。

「②GM_xmlhttpRequest」はこの先の「Greasemonkey API」で詳しく解説しますが、バックグランドで他のウェブページと通信を行ない、ページの内容を取得するGreasemonkey専用の関数です。たとえば、GM_xmlhttpRequestを悪用すると、今見ていないページの情報を盗むことができてしまうので要注意です。

「③無関係なページのURL」が書いてあれば、盗んだ情報を送信する目的で使われている可能性があります。盗んだ情報の送信方法は多数ありますが、大抵どこかに用意したウェブサイトでこっそり受け取っているので、無関係なページのURLは特に注意です。

「④難読化」とはスクリプトが普通には読めないようになっている状態のことです。たとえば上記で紹介したdocument.cookieやGM_xmlhttpRequestを検索されても大丈夫なように、あらかじめコードを暗号化しておくことが可能です。大抵の場合、一見無意味な文字列が相当量を占めていることが多いです。このような場合、悪意のあるコードを隠している可能性が高いと言えます。

以上四点のチェック項目がありましたがいかがでしょうか？　この四点を全部押さえておけばそうそう被害にあうことも考えづらいのですが、セキュリティに「絶対」は無いので過信は禁物です。被害にあわないためにも、できるだけ怪しいスクリプトには近付かないように普段から心がけておきましょう。