COLUMN
米国インターネット事情

Web Bugとプライバシー問題

前川　徹　早稲田大学国際情報通信研究センター
E-mail: tfm@zf6.so-net.ne.jp

Web Bugが急増中

インターネットの商用利用に関するコンサルティングやウェブサイト分析を専門とする米Cyveillanceは2001年8月14日，インターネット利用者のプライバシーを侵害する恐れのある「Web Bug（ウェブバグ）」を埋め込んだウェブサイトが急増しているという調査レポートを発表した（このレポートは，http://www.cyveillance.com/ からダウンロードできる）．このレポートによれば，Web Bugを用いたウェブサイトの割合は，1998年7月の0.664%から2001年7月には3.906%になっている．また，有名ブランド50社のうち8社が，自社のウェブサイトでWeb Bugを用いているという．

このWeb Bug自体は違法ではないし使用方法によっては無害なので，排除すべきものであるとは一概に決めつけられないのだが，Cyveillanceのレポートは「世間での関心が高まるにつれ，企業がウェブを使って許可なくネット利用者の情報を収集しているという事実は，ますます議論になるだろう．したがって，利用者のプライバシーに関する権利と顧客情報収集の必要性のバランスを注意深くとることが企業にとって望ましい道である」と述べている．

Web Bugとは何か

Web Bugについては，2000年夏にも話題になったので説明の必要はないかもしれないが，簡単に仕組みを説明しておこう．

Web Bugは，プログラムミスを意味するバグではない．bugは小さな昆虫や虫のことであるが，俗語では「隠しマイク」という意味があるので，ウェブページに仕掛けられた隠しマイクという意味なのだろう．その見た目や機能から，Clear GIF，Beacom GIF，Web beacomなどと呼ばれることもある．

一般的には1ピクセル（1×1ピクセル）のGIF画像で，ページのバックグランドと同じ色をしていることが多い．つまり，ディスプレイに表示されても何も見えない．問題は，この画像データはそのウェブサイトとはまったく別のサイトに蓄積されていたり，アクセス履歴など利用者に関する情報を収集するHTMLコードが付属していたりする点にある．

つまり，ネット利用者がWeb Bugが埋め込まれたA社のウェブページにアクセスすると，B社のサイトから見えないGIF画像が呼び出されることになり，この時，B社は利用者に知られることなく，利用者に関する情報を収集することができるのである．収集される可能性のある情報は，利用者のIPアドレス，そのWeb Bugが埋め込まれているページのURL，Web Bugの位置，そのページが読み出された日時，パソコンのOS，ディスプレイの解像度，ブラウザの種類やバージョン，直前に設定されたクッキーの情報などである．そもそも，ウェブサーバはコンテンツのリクエストを受け付ければ，リクエストした利用者情報を記録するようになっているので，基本的に利用者のIPアドレス，OSやブラウザの種類といった情報は収集できるし，JavaScriptなどを用いてさらに詳細な情報を収集することも可能である．

Web Bugを用いている企業の代表例は，インターネット広告やマーケティングをビジネスにしている企業である．クライアントのウェブページにWeb Bugを埋め込めば，どのページが最も頻繁に読まれるのか，どのタイミングでどのページが呼び出されるのかを調べることができる．

ちなみに，利用者に関する情報を収集するという目的からすれば，技術的にはGIF画像を1ピクセルにしたり，ページの地の色と同じにする必然はない．バナーやボタンのようにページに明示的に表示してWeb Bugの機能を持たせることも可能である．画像を見えなくしているのは，Web Bugを埋め込んだ人（企業）が見えない方がよいと考えているからである．

Web Bug対策は可能か

Web Bugは別に特殊な技術を使用しているわけではない．利用者のIPアドレスやOSやブラウザの種類などの基本的な情報は，CGIプログラムを書かなくてもサーバの管理者なら簡単に得られるし，わざわざ利用者から見えないGIF画像を用いる必要もない．Web Bugの問題は，利用者がアクセスしたウェブページの企業とは別の企業が，利用者に何も知らせることなくそうした情報を収集している点にある．

もちろん利用者側でWeb Bugの機能を封じることは可能である．たとえば，ブラウザの設定でクッキーを拒

否するようにしておけば，クッキーの情報を盗まれることはない．さらに画像表示をオフにすればWeb Bugの機能を完全に封じ込めることができる．

しかし，クッキーを拒否するように設定すると，利用者IDを何度も入力しなければならなくなったり，利用者識別に基づくリコメンデーションサービスやショッピングカート機能，アマゾン・ドットコムの1-Clickショッピングなどのさまざまなサービスを享受できなくなる．それほど数は多くないが，クッキーを拒否する設定になっていると利用できないサイトもある．まして，画像をオフにしてウェブを利用しようというユーザはいないだろう．

電子メールも追跡できる

Web Bugの本質は，利用者情報を収集するためのHTMLコードである．とすれば，Web Bugを埋め込む対象はウェブページに限定されない．最近，HTMLメールの利用が増えているが，これに埋め込むこともできる．相手がインターネットに接続された環境で，Web Bugを埋め込んだHTMLメールを開くと，埋め込まれたWeb Bugの見えない画像を取り込むために指定されたサーバにアクセスすることになる．つまり，いつ，どこで（といってもサイバースペース上での場所であるが）そのメールが読まれたかを知ることができる．「そんなメールは受け取ったことがない」とか「まだメールを読んでいないので」といった言い訳は通用しなくなる．

実際に，この仕組みを利用して電子メールの追跡サービスを行っている企業もある．たとえば，米国のiTraceYou.com（http://www.itraceyou.com/）や韓国のPostel Services（http://www.postel.co.kr/）である．ちなみに，Postel Servicesのサービスは有料であるが，iTraceYou.comは無料で利用できる．最近は電子メール以外にもHTML対応のアプリケーションは広がっている．たとえばワープロソフトとして事実上の標準になっているかのようなMicrosoft Wordや表計算ソフトのExcelなどのアプリケーションによって作成したファイルにもWeb Bugを埋め込める．もちろん，そのパソコンがインターネットに接続されているという条件付きではあるが，Web Bugを埋め込まれたファイルを開けば，即座にその事実は所定のサーバに通知される．それも利用者に気付かれることなく．

これは，社外秘の文書の漏洩を検知する目的で利用できるかもしれない．秘密文書が社外にネット経由で送られ，どこかで開かれれば，即座にそれを検知できる．文書を配布した関係者ごとにコードを変えておけば，誰が漏洩したかまで突き止めることができるだろう．うまく工夫すれば，著作権管理に応用することもできるかもしれない．

解決策はあるのか

「Web Bug対策は可能か」の項で書いたとおり，利用者側の利便性を損なわないで，Web Bugの機能を封じる有効な手段はない．Web Bugを発見するためのソフトウェアも開発されているが，情報収集を目的としない隠されたGIFに警告を出したり，明らかに情報収集をしているWeb Bugを検知できないなどの欠陥が指摘されている．

どうも現時点では，Web Bugを使用するウェブサイト側で一定のルールを守ってもらうしか方法はないように思える．すでにWeb Bugを使用している企業の中には，そのプライバシーポリシーのページでWeb Bugで収集している情報の種類とその目的について説明しているところがある．たとえば，Yahoo! はWeb Bugをそのサイトの内外で使用していることを明らかにしている（Yahoo! のプライバシーポリシーのページ，http://privacy.yahoo.com/privacy/us/，を参照）．

すでに米国では，個人のプライバシーを守る活動をしているPrivacy Foundationが，2000年9月13日に「Web Bug使用ガイドライン（Guideline for Using Web Bugs）」を発表している．このガイドラインの基本は，Web Bug自体を見えるようにし，誰が何のために，どのようなデータを収集しているかを利用者に公開するというもので，次の5項目からなる．

1. Web Bugはディスプレイ上で視認できるように表示する．
2. Web Bugを設定した企業名をそのアイコンで分かるようにする．
3. そのアイコンをクリックすることによって，(1) どのような情報を収集しているのか，(2) 収集した情報を何のために使用するのか，(3) 情報を使用する企業名，(4) クッキーの情報を取得しているかどうか，などを利用者が確認できるようにする．
4. Web Bugによる情報収集を利用者が中断できるようにする．
5. 子供向けのサイトや医療関連のサイト，金融や求人・求職関係のサイト，性に関するサイトなどのセンシティブなサイトではWeb Bugを使用しない．

直ちに個人を特定できるような情報が収集されてプライバシーが侵害される危険性はかなり小さいと思うのだが，知らない間に誰かが情報を収集しているのは気味が悪い．最低限，誰が何のために，どのようなデータを収集しているかを利用者に公開するというルールを守って欲しいものである．

（平成13年8月27日受付）