Google が仕掛けた罠　杉浦隆幸

「広告枠」を売るだけだったインターネット広告に、劇的な変化をもたらしたといわれるグーグルは、2000 年 10 月に、「アドワーズ（**AdWords**）」という「検索連動型」と呼ばれる広告を始めました。検索結果ページの上部や右横に広告が表示されているのを見たことがあるでしょう。あれが　「AdWords」です。

グーグルはさらに 2003 年 12 月、「アドセンス（**AdSense**）」という広告配信サービスを始めました。これは、個人ホームページやニュースサイト、ブログなどの広告枠と、広告出稿先を探す広告主のあいだを取り持つ「広告代理店」のようなサービスです。

ちなみに私は、個人情報の塊である電話帳データを、ウェブ上のサービスに保存するようなことはしていません。スマホは持っていますが、電話帳アプリには何も登録していないのです。よくやりとりする人の連絡先は、**ガラケー**（スマートフォン登場以前の旧来型の携帯電話）**の電話帳で管理**しています。

LINE 親会社は韓国企業ネイバー

アプリを利用している人には、どのような情報が抜き取られているかはわかりません。そこで、アンドロイドのアプリ限定ですが、アプリが裏でどのような情報を抜き取っているかを調査し、無料で公開しているサイトがあります。「Secroid」セキュロイドというサイト（http://secroid.jp/）がそれで、ほとんどのアプリを網羅しています。

~~~~~~~
「secroid」のサービスが 2017 年 2 月末をもって終了されたらしく、現在既にアクセスできなくなっています。
~~~~~~~

この「他人の無線 LAN の MAC アドレスを、所有者に断ることなく収集する」という行為、法に抵触しそうですが、法律関係者は「違法とは言い切れない」としています。**「グレーゾーン」を法規制より先に必要不可欠なものにしてしまうことで規制されないようにする**――といわれるグーグルらしいやり方をしているようです。

WebArchive
これはいわばインターネット上の公共図書館のようなもので、インターネット上にどのような情報が存在し

たかを「資料として」保存しています。
https://web.archive.org/

フィッシング　phishing
~~~~~~~~~~~
〔sophisticated（洗練された）と fishing（釣る）から〕 有名企業などを装い，ネット上で不正に個人情報を入手する詐欺手法。
~~~~~~~~~~~

名簿の買い取りや販売を行うこれらの業者は、個人情報保護法に反していると思われるかもしれませんが、現行の法律では規制することばできません。一定の条件を満たせば、こうした名簿や個人情報データベースを販売できることを、法律が認めているからです。

マイナンバー制度にまつわるセキュリティ上聞題点、4 つ目は、2017 年 1 月スタート予定のマイナンバー情報閲覧システム「マイナポータル」にあります。
「マイナポータル」からは、本人が自分のマイナンバー情報のやりとりの記録をすべて閲覧することができ、自分の情報を、誰が、いつ、どのような目的で利用したのかを確認することができます。
　また、行政機関に保存されている自分の情報を確認したり、自分に関連する行政サービスのお知らせを受けたり、「電子証明書」を使って手続きをオンラインで行ったりと、さまざまな機能やサービスが「マイナポータル」上で提供されるようになる見込みです。
　情報セキュリティの観点で問題になるのは、**「マイナポータル」が、本人のマイナンバー情報がすべて集まる情報の集積地**になること、そして**インターネットに直接接続している全国民の情報が見られるシステム**であることです。

「スタックスネット（stuxnet)」と呼ばれたマルウェアの主な感染先は、イランの複数の原子力開発関連施設でした。それらの施設で、数万台のコンピュータが「スタックスネット」に感染したと報じられたのです。当時の報道では、実害は確認されなかったものの、原子力関連施設の制御システムを標的にしていることが明かされ、イラン政府当局は「西側諸国による攻撃」との見方を示しました。
・・・
　それからしばらくすると、さらに驚くべきことが明らかになりました。当初は「実害がなかった」と考えられていた「スタックスネット」ですが、原子力設備を停止させていたことが伝えられたのです。当初「実害がなかった」とされたのは、制御システムの動作を監視するシステムに対し、制御システムが正常に動いているように見せかける細工をしていたからでした。

ここまで高度なマルクエアを開発するには、人や技術、知識だけでなく資金力も必要なはずです。「スタックスネット」の開発には多額の費用がかかっているはずです。

後にフィンランドのセキュリティ企業が発表したレポートでは、アメリカの関与が指摘され、**最初は否定していたアメリカも結局、関与を認めました**。

ライフハック life hack 仕事や生活を便利にする技

たとえば、日本やアメリカは誰でも簡単にレンタルサーバーを借りることができますが、中国はウェブサイトの設立が許可制で、簡単にサーバーを持てるわけではありません。つまり、日本やアメリカでは、その気になれば他国が簡単に「サイバー基地」をつくれてしまうのに対して、中国に「サイバー基地」をつくろうと思っても、サーバーを借りるのは容易ではなく、どこかのサーバーに侵入しなければならないということです。

日本の業界の先行き不透明さと提示された好待遇に、そのとき多くの**日本人技術者が韓国企業に転職しましたが、その後は 1 年、2 年という短期間で解雇**されるケースが少なくなかったようです。引き抜いた企業の側から見れば、一度ノウハウを取り込んでしまえば、給料を払い続ける意味がなくなってしまうからです。

そういう危険なファイルはウイルス対策ソフトがチェックするはずだから大丈夫、と思った人もやはり注意が必要です。**攻撃側は、市販されているウイルス対策ソフトで検知されないことを確認したうえでメールを送りつけている**のです。

2015 年 6 月に、日本年金機構から約 125 万件の年金情報が流出したことが公表されました。このときに仕掛けられたのが「標的型攻撃」で、同年 5 月のうちに断続的に、日本年金機構の複数の職員に対して攻撃メールが送られていたことが明らかにされています。誰がどういう目的でこの攻撃を仕掛けたのか、この情報がどこでどのように使われているのかは、残念ながら解明されていません。

一般論ですが、「標的型攻撃」を仕掛けてくるのは、主に、中国系のハッキング組織と考えられでいます。**日本企業や日本政府の情報に中国共産党が懸賞金をかけていて、それ目当てに攻撃を仕掛けてくる**と見られています。

ファイルを開いた瞬間、そのパソコンはウイルスに感染してしまうわけですが、見た目にはファイルが開く以上のことは起こらず、たいていの場合はウイルス対策ソフトもウイルスだと検出できないため、ウイルス感染に気づくのは簡単なことではありません。

このときパソコンに感染するウイルスは、それ自体が悪さをするというよりも、外部からそのパソコンを遠隔操作できるようにする「遠隔管理ツール（Remote Administration Tool: **RAT**）」というウイルスをダウンロードしてくることに特化したものです。

このように、何食わぬ顔をして攻撃対象内部の情報システムやコンピュータに忍び込むウイルスのことを、「トロイの木馬」と呼びます。

「IP アドレス」の割り当て情報は公開されており、WHOIS というサービスにより誰でも検索することができます。その先は、日本国内からのアクセスであれば、捜査機関がプロバイダや携帯電話会社に照会すると、問題の「IP アドレス」を使用していた契約者を突き止めることができるのです。

〜〜〜〜〜〜〜〜〜

ドメイン/IP アドレス サーチ 【whois 情報検索】

https://www.cman.jp/network/support/ip.html

〜〜〜〜〜〜〜〜〜

「プロキシサーバー」の「プロキシ（proxy）」とは、日本語で「代理人」を意味します。「代理人」が本人に代わってさまざまな法律行為を行うように、「プロキシサーバー」は自分のコンピュータの代わりに通信を行います。

「代理」という言葉でイメージが湧きにくければ、「接続中継」という言葉で理解したほうがわかりやすいかもしれません。インターネット上のあるサービスにアクセスする際、自分のコンピュータから直接アクセスするのではなく、**「プロキシサーバー」（接続中継サーバー）**にまずアクセスして、そこから目的のサービスにアクセスします。そうすることによって、目的のサービスを提供しているサーバーから見れば、「プロキシサーバー」の IP アドレスからアクセスがあるように見えるため、本来の IP アドレスを見えないようにすることができます。

インターネット上のコンテンツやサービスには、世界中のどこからでもアクセスできると思っていませんか？　あるいは世界のどこにいても、同じ内容が表示されると思っていませんか？　現実はそうではありません。法律の違いやその他さまざまな理由で、アクセスできる国を制限しているコンテンツやサービスが少なくなく、また**同じ URL を入力しても、国によって表示される内容が違うことがある**のです。その際、アクセス元の地域の判定には IP アドレスが使われています。

「**Tor**」と呼ばれる匿名化手段を使う方法があります。

ここでは技術的な説明は省きますが、そのひとつの特徴は、最低 3 カ国を経由して目的のサーバーにアクセスすることになるため、オリジナルのアクセス元の IP アドレスは、

ほぼ明らかになりません。
　原理的には追跡可能なのですが、経由国すべての捜査協力が必要なうえ、「Tor」で中継されるサーバーではログ（記録）を取っておらず、他の手段で「Tor」の通信を特定し記録しておくことが必要で、膨大な手間や資金、そして協力体制が必要です。解決されていない**サイバー犯罪の多くが、この「Tor」を隠れ蓑**として使っていると推測されます。
・・・
たとえば、発信する情報が米国政府の諜報網に
かからないようにするために、メディア関係者が使っていたりするのです。興味のある方は、「Tor」で検索してみてください。公式サイトから容易に日本語版を無償で人手できます。

フェイスブックの規約やプライバシーポリシーに従えば（利用している以上従っていることになります)、一度投稿した情報は、設定レベルにかかわらず、**誰がどう使ってもいいことになっています**。

シークレットモード
　ブラウザをシークレットモードで使用すると、開いていたタブやウインドウをすべて終了するとき、クッキーが破棄されて、通常のブラウザでは追跡できない状態になります。

アドブロック・プラス
　アドブロックは、サイト運営者に対し、広告を控えめにすることを求めています。そして、賛同する業者を「控えめな広告を許可」するリストに入れ、広告企業に費用を要求しています。

グーグルマップを開き、「メニュー」→「タイムライン」をクリック。そこにあなたのこれまでの行動記録が記されているはずです。時間の記録や、店名まで明らかになっていたりするので、驚かれるかもしれません。