重　要

コンピューターウイルス「DNS Changer」

緊急報告書

IEAS 管制センター統括グループ

グループ統括：白原　信吾

コンピューターウイルス「DNS Changer」に感染したパソコン（PC）は、米国時間2012年7月9日にインターネット接続ができなくなる恐れがあることがSIATORUコントロールより報告がありました。世界での感染数はおよそ400万件と思われます。岡山本部IEAS国際ネットワーク管理統括センターによる報告では、日本国内でどれほどのPCが被害にあっているか、つかめていない状況です。

DNSの設定が勝手に書き換えられていると考えます。

「DNS Changer」に感染すると、PCやルーターのDNS設定が勝手に書き換えられ、「j-cast.com」のIPアドレスを問い合わせる先が不正なDNSサーバーとなり、正しいIPアドレス情報が与えられない為、代わりに攻撃者にとって都合のよい別のサイトに誘導されてしまう現象が見られる。2011年11月9日の米連邦捜査局（FBI）の発表によると、2007年以降このウイルスに感染したコンピューターは、世界各地で約400万台に上ったとの報告があります。個人だけでなく、米航空宇宙局（NASA）のような政府機関も含まれていたと言う報告。既に攻撃の首謀者は拘束されており、米当局が不正なDNSサーバーを撤去して別のサーバーに入れ替えたと報告されています。サーバーを突然ストップすると感染したままのPCやシステムが影響を受ける可能性があるとして運用が続けられていたが、最終的には米国時間2012年7月9日に停止することが決まったとの報告が上がりました。FBI公式ブログによるとウイルスに感染したPCは、代替DNSサーバー停止後にネット接続不可となる恐れがあるという。設定していたDNSサーバーが動かなければ、ドメイン名からIPアドレスを調べられない。米国内ではおよそ6万4000人のユーザーが、7月9日になってネットに接続できなくなる可能性があると、FBIでは推測しています。日本国内の状況は、独立行政法人・情報処理推進機構（IPA）による報告では、「感染者がどの程度いるのか、現状では不明です」との事です。

ウイルス使った「違法広告」で11億円荒稼ぎの可能性。

感染経路も不明な点が多い。ウイルスがメールに添付されて、うっかり開くと感染するケースはよく耳にするが、IPAによると「DNS Changer」に関しては「そのような報告を聞いていません」との報告です。そのため、ウェブサイト上にウイルスが仕掛けられていると思われます。そこを訪れて感染する可能性もあるとの報告です。必ずしも、わざわざつくられた悪意のあるサイトとは限らず、通常閲覧するようなサイトでウイルスにかかるケースも想定されています。「DNS Changer」では、ユーザーが閲覧したいサイトを開こうとしても、攻撃者の悪意によって明らかに違う別の不正サイトに導かれてしまう為、感染の有無は一見分かりやすいですが、「例えば感染したPCで大手ポータルサイトを開こうとしたら、そのポータルにそっくりだが悪意のある不正サイトに持っていかれるということも考えられます」（IPA）。FBIの報告では、攻撃者がウイルスによる「違法広告」で1400万ドル（約11億円）以上を荒稼ぎしていたという報告です。広告を使った「悪事」の詳細が分からず推測の域を出ないが、仮にユーザーが感染

しているPCを使って、あるサイトにアクセスを試みたとき、該当サイトを開かせたうえで違法広告をポップアップで出す、あるいはいったん違法広告のページに飛ばした後に正しいサイトに移動させる、といった手口も考えられています。ネットセキュリティー団体はサイト上に、「DNS Changer」の感染チェックページを設けており、IPAでも利用を勧める方針です。万一、感染が明らかになったら「最新のウイルス対策ソフトで、PCやルーターを点検してほしい」と促すとの報告です。では感染の有無を確かめないまま「その日」を迎え、急にネット接続が不可能と対処法。理論的には、書き換えられているDNS設定を正しいものに戻す。しかし「ウイルスを駆除できていないと、正常なDNS設定にしてもまた不正な設定にいつの間にか切り替わってしまう可能性も確認されています」とIPAでは懸念する。国内の報告事例がほぼゼロということもあってつかみどころがなく、何とも不気味なウイルスと発言されている。我々も米国を除き、全世界でも報告事例がほぼゼロであるとの報告とあってつかみどころがありません。緊急調査を実施する事を許可を頂きたい。