

2007年8月23日

JPドメイン名諮問委員会
委員長 後藤 滋樹 殿

株式会社日本レジストリサービス
代表取締役社長 東田 幸樹

諮 問 書

フィッシングは、インターネット利用者の安心・安全を脅かす行為のひとつであり、その被害は増加しています。その対策として、被害に遭わぬようインターネット利用者に対して情報提供や注意喚起などを実施することはもちろんですが、フィッシングに使われているWebサイトを使用停止することや、フィッシングを行っている者を特定し、取り締まることなども並行してなされる必要があります。

Webサイトを使用停止する方法のひとつとして、そのURL(Webアドレス)に含まれるドメイン名の登録を取り消す等により、ドメイン名自体を使用停止とすることが考えられます。一方、ドメイン名レジストリは、ドメイン名の文字列の意味やその使用方法には関与しないという原則があります。このため、使用方法が不適切であることを理由に、レジストリが独自の判断でドメイン名を取り消すことは行っていません。しかし、ドメイン名に関する情報を持ち、ドメイン名をインターネット上で使用可能とするためのDNSを運用しているドメイン名レジストリは、指定事業者やISPと連携して、フィッシング被害防止に一定の役割を果たしうることも事実です。

このような状況を踏まえ、健全なインターネット利用促進に資するという観点から、フィッシング被害防止においてドメイン名レジストリが担うべき活動の方針についてご答申いただきたく、諮問いたします。

諮問理由

近年、インターネットは日常生活に不可欠なインフラとしての機能を増しており、金融機関やショッピングサイトの利用等経済活動も拡大しています。その一方で、フィッシング等、インターネット利用者の安心・安全を脅かす行為が増加し、その手口も巧妙化しています。

フィッシングとは、例えば、多くの一般消費者に金融機関を装った電子メールを送りつけ、電子メールを受信した消費者がそこに記されたWebサイトにアクセスして金融機関の暗証番号などを入力するよう巧妙に仕向け、個人情報などを騙し取るといった行為です。URL (Webアドレス) は情報発信元であるWebサイトの場所を示すものですが、そのURLの一部としてドメイン名が含まれています。あるURLが悪質な行為を行っているWebサイトを指している場合、そのURLを使えなくするために、そこに含まれるドメイン名を使用停止とすることが対策のひとつとして考えられます。

フィッシングへの取り組みの主なものとして、関係団体を中心に「フィッシング対策協議会」が設置され、そこでは、フィッシングに関する情報収集・提供、事業者間の情報共有、一般利用者への注意喚起等の活動が行われています。他の活動としては、「国民のための情報セキュリティサイト」にて、インターネットに潜む犯罪などに対する具体的なセキュリティ対策等についての注意喚起や、一般利用者がなすべきことの解説などが公開されています。ISP等が中心となった「フィッシング対策推進連絡会」では、情報共有するとともに、効果的な対策について検討しています。また、国境を越えたフィッシングも数多くあることから、国際的な協力活動としてAnti-Phishing Working Groupが米国に設置されており、そこでは、フィッシング等を防止するため、業界をまたがった世界的な対策が検討されています。フィッシング対策に関連した主な機関を以下に紹介しますが、これらの機関における活動は、フィッシング詐欺に遭わぬようにというインターネットユーザへの啓発が主なものとなっています。

- ・ 経済産業省の「フィッシング対策協議会」
<http://www.antiphishing.jp/index.html>
- ・ 総務省の「国民のための情報セキュリティサイト」
http://www.soumu.go.jp/joho_tsusin/security/index.htm
- ・ 総務省の「フィッシング対策推進連絡会」
http://www.soumu.go.jp/s-news/2005/050810_4.html 等
- ・ Anti-Phishing Working Group
<http://www.antiphishing.org/>
- ・ JPRSからのフィッシング対策関連動向の紹介
<http://jpinfo.jp/event/2007/0723ICANN1.html>

JPRSに対しても、海外のインターネット関連機関や一般のインターネット利用者から「JPドメイン名を使ったWebサイトでフィッシングが行われているので、早急に対処して欲しい」という要求がなされることがあります。このような場合、JPRSは当該ドメイン名を管理している指定事業者と連絡を取り、さらにその指定事業者

が当該ドメイン名の登録者と連絡を取り、ドメイン名の悪用をやめるように要求することにより解決しています。

さらに強硬な手段として、レジストリであるJPRSが当該ドメイン名を使えなくする措置を実施すべきである、という意見もあります。しかし、次の理由により、悪質な使用がなされているドメイン名をレジストリ独自の判断で使用停止とすることはしていません。これは、諸外国のレジストリでも同様の状況です。

- レジストリは、ドメイン名が世界で一意的文字列となるように登録者からの申請を処理し、それをインターネット上で使用可能とすることを役割としているため、ドメイン名の文字列の意味やその使用方法には関与せず、第三者機関にて何らかの有効な判断がなされた場合は、それに従う。
- ドメイン名登録者に対する各種サービスは指定事業者が提供しているため、指定事業者の頭越しにレジストリが登録者のドメイン名を使用停止とすることは適切でない。
- 1つのドメイン名がいくつかのURLやメールアドレスで使われている場合、そのドメイン名を使えなくすると、悪質な使用のみでなく、そのドメイン名を使っているすべての通信が不可能になってしまう。

また、仮にあるドメイン名を使用停止とする対処をとったとしても、その効果には、次のような限界があります。

- WebブラウザはDNS情報を使って所定のWebサイトにアクセスする。このアクセスにおいては、通常、大元のDNS情報を参照する代わりにキャッシュ(ISP等がローカルに持っているDNS情報のコピー)を参照する仕組みが使われており、そのキャッシュは最大24時間更新されない。したがって、大元のドメイン名・DNS情報の削除は即効性がないことが多い。すなわち、フィッシングサイトが開設されてから数時間以内での初期被害はドメイン名の取消やDNS情報の削除では防げないことが多いということになる。
- フィッシングにおいては、多くのドメイン名を登録して多くのURLを作り、それらすべてがフィッシングサイトを指すという手法が用いられるようになってきた。このため、1つのドメイン名を取り消したとしても他のドメイン名を使ったURLでそのフィッシングサイトに誘導することができるため、効果が限定的である。

しかし、ドメイン名のDNS情報を使用不可とすることやドメイン名自体を取り消すことは、当該ドメイン名の悪質な使用を将来にわたって防止できるという大きな効果があります。ISPやWebホスティング事業者、その他セキュリティ関連機関等と協力して、ドメイン名の使用可否に関する対処も含めたフィッシング対策に取り組むことにより、ユーザの教育・啓発という防衛的な対策のみでなく、特定のフィッ

シング活動を不可能とするという積極的な対策も可能となります。危険度や実害が増加していることを考慮すると、このようにフィッシング活動を積極的に抑止することは社会的要請であると考えられます。すなわち、適切な条件の下、ドメイン名レジストリがドメイン名を使用停止とすることができれば、それは、健全なインターネットの発展に資するものとなります。

関連機関の協力によりフィッシング対策を行う場合、特に次の点を考慮する必要があります。

- どのような事象をフィッシングであると判断するのか、判断することは可能か。
- 個別の事象がフィッシングであるか否かを誰が判断するのか。
- 個別の事象がフィッシングであるか否かを判断するための第三者機関にはどのようなところがあるか。
- フィッシングを止めるにはどのような方法があり、どれが有効か。
- ドメイン名の使用停止の条件として、ドメイン名の使われ方を理由とするのは妥当か。
- 個別のドメイン名の使用停止を判断するのは誰か。
- レジストリがドメイン名の使用停止を実行するための適切な手順は何か。

上記を勘案し、JPRSがドメイン名レジストリとして実施すべきフィッシング対策についてご答申いただきたく、諮問いたします。

以上