2007年8月23日
第21回JPドメイン名諮問委員会
資料4

フィッシングへの対策について
～レジストリの観点から～

2007年8月23日

株式会社 日本レジストリサービス

検討のポイント

1. 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
2. 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
3. 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
4. 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
5. 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
6. 個別のドメイン名の使用停止を判断するのは誰か
7. 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

1. 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

- フィッシングの定義
  - フィッシング（Phishing）とは、金融機関（銀行やクレジットカード会社）などを装った電子メールを送り、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を詐取する行為である。電子メールのリンクから偽サイトに誘導し、そこで個人情報を入力させる手口が一般的に使われている。

    出典：フィッシングとは(フィッシング対策協議会)
    http://www.antiphishing.jp/doc/aboutphishing.html
- フィッシングであると判断する要件
  - 以下の全ての条件を満たす場合はフィッシングである可能性が高い
    - ① 金融機関（銀行やクレジットカード会社）などを装った電子メールが送られてきた
    - ② 電子メールに書かれていたWebサイトが金融機関のWebサイトととてもよく似ている
    - ③ 住所、氏名、銀行口座番号、クレジットカード番号などの個人情報の入力欄がある
  - ただし、上記の①と②は明確に判断することが難しいため、一般にフィッシングか否かを判断することは困難

2. 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

- 想定される組織
  - レジストリ
    - レジストリの本来の役割から逸脱し、ドメイン名の使用方法に関与することになるため、単独で判断することは避けるべき
  - 指定事業者
    - 通常、単独で判断するのは困難
  - 信頼できる第三者機関
    - バランスの取れたメンバーで構成される必要がある

3. 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

- 「第三者機関」の例
  - 裁判所
    - 法的効力は十分にあるが、判断が出るまでに時間がかかる
  - 警察
    - 取り締まりを行うためには法制度化が必要
  - JPCERT/CC＊など
    - どこまで権限を与えられるか
  - 政府が主催するセキュリティ関連団体(協議会、委員会など)
    - レジストリも参加した上で、第三者機関の設立を働きかける必要があるか
  - レジストリが設置する第三者委員会
    - 公平性・中立性を担保するための仕組みが必要

＊インターネットを介して発生するコンピュータセキュリティに関連する事象の情報を収集し、インシデント対応の支援、コンピュータセキュリティ関連情報の発信などを行なう組織。
出典：IT用語辞典 e-Words
http://e-words.jp/w/JPCERT2FCC.html

4. 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

- フィッシングを止める代表的な方法
  - フィッシングに使われているドメイン名を使用停止とする(ドメイン名の削除、ドメイン名のネームサーバ削除など)
    - フィッシングの大元をとめることが出来る
    - DNSの仕組み上、即効性がない
    - フィッシングサイトだけでなく、そのドメイン名を使っている全てのWebサイトやメールアドレスが使用不可能になる
  - フィッシングサイトを使用停止とする(サーバ撤去、コンテンツ削除など)
    - 即効性がある
    - 指定事業者・ISPと連携して対応する必要があり、即時に使用停止とすることは困難
    - ドメイン名は残るため、別の指定事業者・ISPを利用して別のフィッシングサイトを立ち上げることが可能
  - フィッシングサイトの運営者を取り締まる
    - 同じ運営者によるフィッシングサイトの立ち上げを抑止できる
    - 別途、Webサイト自体の削除作業を行う必要がある

5. 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

- 使われ方を使用停止の理由とする
  - レジストリの本来の役割からは逸脱する
  - 使われ方が正しいか否かの一般的な基準を作るのは困難

- 使われ方を使用停止の理由としない
  - レジストリの本来の役割に沿った対応となる

6. 個別のドメイン名の使用停止を判断するのは誰か

- 判断者として想定される組織
  - レジストリ
    - 第三者機関での「フィッシングである」との判断に基づき、ドメイン名の使用停止をほぼ自動的に判断するのが望ましい
  - 指定事業者
    - サービス約款に「フィッシングと判断する場合はドメイン名を使用停止とするようレジストリに申請する」と記し、それに基づきレジストリにドメイン名の廃止を届け出ることは可能
  - 信頼できる第三者機関
    - フィッシングであるか否かの判断は可能だが、ドメイン名の使用停止が有効な事例か否かを判断するには、バランスのとれた判断プロセスが必要

7. 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

- レジストリと指定事業者で連携して対応
  - 第三者機関からの指摘があった時点で確認を行うなど、密に連携をとりながら対応する
    - レジストリ側で使用停止を実行する前に、指定事業者側でも同様の作業を実施することが可能
  - 確認や予告などは行わず、使用停止時に指定事業者にその旨の通知を行う
    - レジストリ側の責任は果たしているが、指定事業者が登録者との間にトラブルを抱えやすい

- 指定事業者との連携は行わない
  - 予告も使用停止時の通知も行わない
    - 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の使用停止を行うことになり、指定事業者は使用停止の事実を発生時に把握できないため、適切でない