ブラウザ搭載フィッシング検出機能の
検出精度に関する調査

2010 年 4 月 22 日
フィッシング対策協議会

1. はじめに

1.1 背景

フィッシング対策協議会および JPCERT コーディネーションセンター(以降、JPCERT/CC とする）に報告されるフィッシングサイトの件数をみると、2009 年 5 月より日本のブランドを狙ったものが急増している。これらの急増するリスクの低減策には様々なアプローチがある。ユーザがアクセスしようとする URL をあらかじめ用意したブラックリストと比較し、必要に応じてアクセスを遮断するフィッシング検出機能もその 1 つである。現在主要なブラウザにはこのフィッシング検出機能が備わっており、被害防止に役立っていると考えられているが、その検出精度について日本のブランドを騙るフィッシングサイトの URL を使用して検証したデータはない。

2009 年 12 月に JPCERT/CC が行った事前調査によると、主要 3 ブラウザを用いて PhishTank（フィッシング URL の公開データベース）から取り出した URL を 20 件のフィッシングサイトの URL を判定させるとおよそ 18～19 件をフィッシングサイトとして検知する。対して、フィッシング対策協議会および JPCERT/CC に報告される日本のブランドを騙るフィッシングサイトの URL 25 件を判定させると、フィッシングと検知できるものはわずかに 3 件であった。また一度フィッシングとして検知されていた URL が時間経過と共に検知されなくなるなどの事象も確認された。

この事前調査の結果から、以下の二つの仮説が導き出せる。

- 仮説 1 : 現在のブラウザ搭載フィッシング検出機能は、特に日本のフィッシングサイトへの対応が遅れている
- 仮説 2 : ブラウザ搭載フィッシング検出機能は製品ごとに細かな挙動や更新タイミングの違いがあり、正しく使用しないと十分に機能しない

1.2 目的

本調査は、1.1 で示した仮説を検証し、現在のブラウザ搭載フィッシング検出機能の性能を正しく理解することを目的とした。また、その結果検出機能が十分でない場合には、その改善に向けた取り組みの提案を行うこととした。

具体的には、さまざまな手段で入手したフィッシングサイトの URL を実際にフィッシング検出機能を用いて判定し、検出能力を測定した。

2. ブラウザのアンチフィッシング機能について

2.1 Internet Explorer 7 およびInternet Explorer 8

昨今のフィッシング被害の増加を受け、Microsoft社は 2006 年にリリースしたWindows

XP Service Pack 2 のInternet Explorer 7 からアンチフィッシング機能を搭載している。Microsoft社のWebサイトの情報によれば[1]、特許出願中である「ビルトインフィルタ」によって、表示するWebアドレスおよびWeb ページをスキャンすることで、既知のオンラインWeb詐欺やフィッシング詐欺に関連する特徴を探し、そのWebサイトに詐欺の疑いのある場合は、警告を表示すると記述されている。そのため、既知の悪質なWebサイトの閲覧をブロックするためのURLブラックリスト以外にも、詐欺サイトの兆候の有無を判断するための何らかの検知アルゴリズムを使用していると思われる。なお、検知アルゴリズムの詳細やURLのブラックリストを更新するタイミングなどについては、2010 年 2 月現在においてMicrosoft社から公開されていない。

URL のブラックリストは、Microsoft 社が独自に管理しているリストと思われる。また、Internet Explorer 8 からは「SmartScreen」と呼ばれる機能が搭載された。これは、Internet Explorer 7 のアンチフィッシング機能に不正なプログラムのダウンロードを検知する機能が追加されたものである。そのため、不正プログラムのダウンロード対策についてはInternet Explorer 8 の方が強力であるが、ことフィッシングサイトの検知に関しては、基本的に Internet Explorer 7 と Internet Explorer 8 では同様と考えられる。

2.2 Mozilla Firefox 3

Mozilla Firefoxについては、Mozilla Firefox 3 からフィッシング詐欺やマルウェア対策機能が追加された。Firefoxの開発元であるMozillaのWebサイト[2]によると、フィッシング詐欺サイトとして報告されているサイトを開いてしまった場合に、警告を表示すると記述されている。判定に必要なURLのブラックリストは、Google社の「Safe Browsing API」を使用している。Google社のSafe Browsing APIのWebページ[3]にもFirefoxが利用していることが記述されている。

2.3 Safari 4

Safariについては、Safari 3.2 からフィッシング対策機能が追加された。Apple社のWebサイト[4]によると、フィッシングやマルウェアが含まれる可能性があるWebサイトにアクセスすると、閲覧者に自動的に警告し、ページが開かないようにする仕組みであると記載がある。通常は表示されないが設定画面において、ある条件の時に表示される警告メッセージなどから、Google社のSafe Browsing APIを使用していると推察される。

3. アンチフィッシング機能を比較するツール

3.1 システム概要

1000 件を越すフィッシングサイトの URL の検知性能を測定するために、作業の自動化は欠かせない。ここでは複数のブラウザのアンチフィッシング機能の性能の検証作業の自動化を実現するために開発したシステムについて解説する。システムは、URL データと Tool 設定ファイルを入力とし、比較対象となる 3 つのブラウザ、Internet Explorer、Firefox、Safari の各プログラムに渡し、結果を CSV ファイルに出力する仕組みを有する。作成した

[1] http://www.microsoft.com/japan/protect/products/yourself/phishingfilter.mspx
[2] http://mozilla.jp/firefox/phishing-protection/
[3] http://code.google.com/intl/ja/apis/safebrowsing/developers_guide.html
[4] http://www.apple.com/jp/safari/features.html#security

比較ツールは、以下の基本機能を有する。

- ブラウザ起動と URL の入力
  比較対象とする 3 つのブラウザ(Internet Explorer、Firefox、Safari)を順番に起動し、調査を行う Web ページの URL を入力する。

- タイトルバーの検証
  入力した URL を表示した際、ブラウザのタイトルバーにどのような文字列が表示されるかを監視し、以下の 4 つのパターンに分類する。

  ①フィッシングサイトを検知した際の警告文字列：Detect
  ②404 や 403 などのコンテンツが存在しない場合の文字列：404
  ③何らかの問題により文字列が取得できない場合：Error
  ④その他のメッセージ文字列を取得した場合：Clean
  ブラウザのアンチフィッシング機能でブロックされた場合は、①のパターンに分類される。

- 結果の出力
  検証結果をファイルに出力する。

4. アンチフィッシング機能の比較実験

4.1 実験概要

本実験は、3 章で述べたアンチフィッシング機能の比較ツールを用いて、Internet Explorer 7、Internet Explorer 8、Firefox3.5、Safari4 の 4 つのブラウザの検出結果にどのような違いが生じるかについて検証したものである。以下、実験の概要について述べる。

(1) 実験で使用するデータ

今回の実験では、以下の 3 つのソースから取得したデータ(フィッシングサイトの URL)を使用し、ブラウザごとの判定精度や傾向について明らかにする。

(a) PhishTankを情報源とするフィッシングサイトのURL

PhishTank は、コミュニティによって収集された既知のフィッシングサイトに関する URL のリポジトリである。この Web サイトに保存されている URL1,000 件(収集期間: 2010/1/25～2010/1/29)を使用して各 URL に対して 5 日間（調査期間：2010/1/25～2010/2/5）検証を行う。

(b) JPCERT/CCを情報源とするフィッシングサイトのURL

JPCERT/CC が収集した、国内外から報告され、JPCERT/CC により 100%フィッシングサイトと確認された URL305 件（収集期間：2009/12/1～2010/1/29）を使用して 5 日間(調査期間：2010/2/2～2010/2/8)検証する。

(c) セキュアブレインを情報源とするフィッシングサイトのURL

㈱セキュアブレイン社が収集した、国内外から報告され、目視により 100%フィッシングサイトと確認された URL29 件(取得期間 : 2010/1/2～2010/2/5)を使用して 5 日間(調査期間 2010/2/1～2010/2/12)検証する。

(2) 判定結果の分析方法

判定結果については、以下の基準により分析を行う。
3.1 において述べたように、比較ツールはブラウザのタイトルバーに表示される文字列を監視し、結果を以下の 4 パターンに分類する。

Detect / 404 / Error / Clean

これら 4 パターンの振り分けイメージを図 4.1-1 に示す。

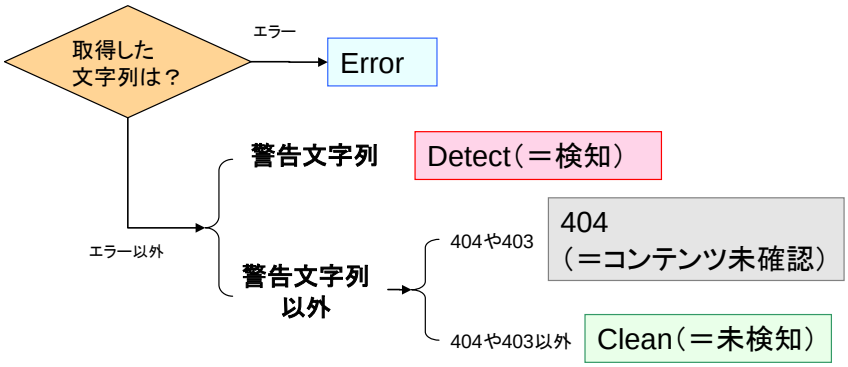

図 4.1-1 検証結果の判定イメージ

図 4.1-1 で記載した、「検知」、「コンテンツ未確認」、「未検知」以外に「有効検知」という分類を設ける。

- **有効検知数/有効検知率**
  検知数とコンテンツ未確認数を加算した値を「有効検知数」と定義する。
  今回の実験においては、単純に考えれば、未検知数が少なく、検知数が多いものが優れているとみなすことができる。しかし、ブラウザの判定性能（判定精度）を評価する上で、検知数の多さだけを基準とするのは適切でない。本来 404/403 などと判定されるべき既にコンテンツが削除された URL をフィッシングサイトとして検知（厳密には誤判定）している可能性もあるからである。判定精度を判断するためには、検知数だけでなくコンテンツ未確認数と合わせて考慮する必要がある。このため、検知数とコンテンツ未確認数を加算した値を「有効検知数」と定義する。別の見方をすると、有効検知率はユーザがコンテンツを閲覧できない率（ユーザが安全にコンテンツを閲覧できる率）との見ることもできる。また、有効検知数をサンプル数で割ったものが有効検知率となる。

4.2 結果分析

実験結果について分析を行った。

4.2.1 PhishTank分の実験結果の分析・考察

PhishTank から取得したフィッシングサイトの URL を用いた実験結果についての分析、考察について述べる。

(a) 検知率：1 日当たりの検知数の平均と、検知率は以下となる。

表 4.2-1　PhishTank 分の検知率

	（1000 件中）	IE7	IE8	Safari	Firefox
全データ平均	検知数	210.6	233.4	667.8	746.6
	検知率(%)	21.1%	23.3%	66.8%	74.7%

検知率については、Firefox が最も高く、以下 Safari、IE8、IE7 の順となっていることが分かる。また、IE については、8 の方が若干高いものの、7、8 の両バージョンでほぼ同等の検知率を示している。

(b) 有効検知率：1 日当たりの有効検知数の平均と有効検知率は以下となる。

表 4.2-2　PhishTank 分の有効検知率

	（1000 件中）	IE7	IE8	Safari	Firefox
全データ平均	有効検知数	805.6	818.6	846.6	913
	有効検知率(%)	80.6%	81.9%	84.7%	91.3%

有効検知率については、IE7 が最も低く、以下 IE8、Safari、Firefox の順に高くなっていることが分かる。ただし、表 4.2-1 に示した検知率と比較すると、値の開きが狭まっていることが分かる。特に、IE7、8 と Safari についてはほぼ同等の有効検知率となっている。

(c) 検知率の推移：検知数の推移の観点からデータの抽出を行った。

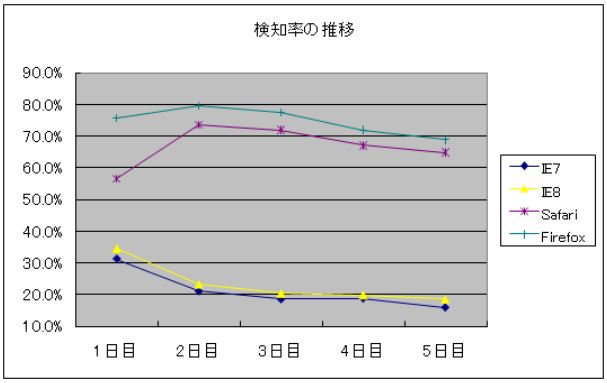

図 4.2-1　PhishTank 分の検知率の推移

図 4.2-1 に示したグラフから明らかなように、IE7、8 と Safari、Firefox とで大きく傾向が分かれている。IE については、1 日目が最も高い検知率を示し、2 日目に 10%程度下がり、その後緩やかに検知率を下げている。一方、Safari、Firefox については、1 日目よりも 2 日目に大きく増加し、その後微減している。

(d) 有効検知率の推移：有効検知率の推移の観点からデータの抽出を行った。

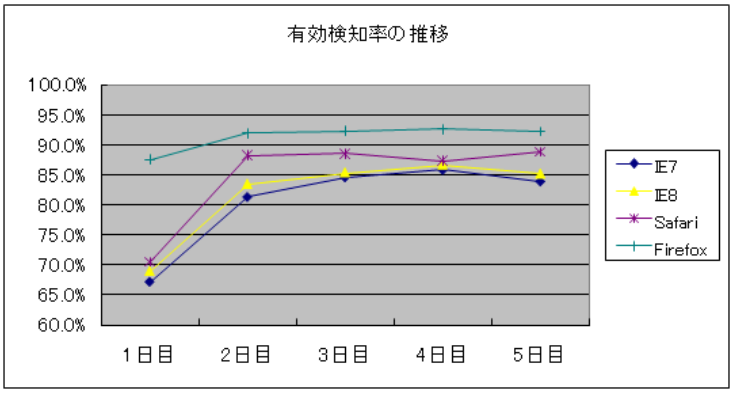

図 4.2-2　PhishTank 分の有効検知率の推移

いずれのブラウザも同様の傾向を示しており、2 日目に増加し、その後はほぼ横ばいに推移していることが分かる。

4.2.2 JPCERT/CC分の実験結果の分析・考察

JPCERT/CC が収集したフィッシングサイトの URL を用いた実験結果についての分析、考察について述べる。前述のとおり、検査データに更新や追加はなく、5 日間同じ 305 件のデータで実験を行った。

(a) 検知率　：1 日当たりの検知数の平均と、検知率は以下となる。

表 4.2-3　JPCERT/CC 分の検知率

（305 件中）	IE7	IE8	Safari	Firefox
検知数	9.8	12.6	81.2	87.2
検知率(%)	3.2%	4.1%	26.6%	28.6%

Firefox が最も高く、次いで Safari、IE8、IE7 の順番となっている。表 4.2-1 に示した PhishTank 分と比較すると、全体的に検知率が大幅に低くなっていることが分かる。

(b) 有効検知率：有効検知数の平均と有効検知率を以下に示す。

表 4.2-4　JPCERT/CC 分の有効検知率

（305 件中）	IE7	IE8	Safari	Firefox
有効検知数	244.8	247.6	224.2	248.2
有効検知率(%)	80.3%	81.2%	73.5%	81.4%

有効検知率については、IE7、IE8、Firefox についてはほぼ同等となっている。

(c) 検知率の推移：検知数の推移の観点からデータの抽出を行った。

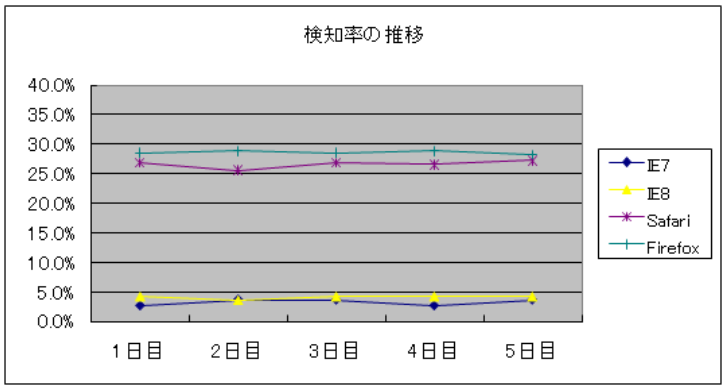

図 4.2-3　JPCERT/CC 分の検知率の推移

図 4.2-3 に示したグラフから明らかなように、IE7、8 と Safari、Firefox とで傾向が分かれている。IE については、3～5%の間でほぼ横ばいに推移している。Safari、Firefox については、25～30%の間でほぼ横ばいに推移している。

(d) 有効検知率の推移：有効検知率の推移の観点からデータの抽出を行った。

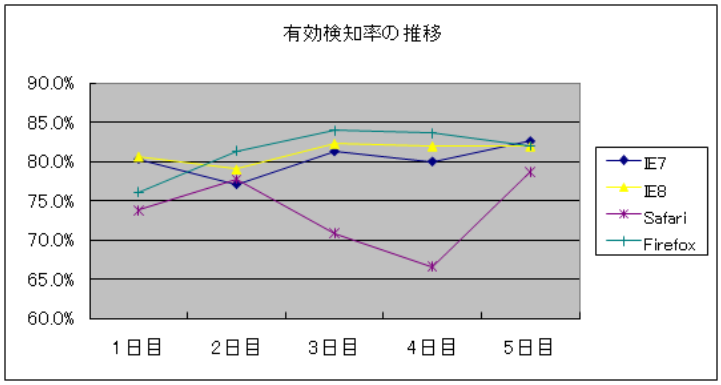

図 4.2-4　JPCERT/CC 分の有効検知率の推移

図 4.2-4 に示したグラフから明らかなように、Safari を除いていずれのブラウザも同様の傾向を示しており、75～85%の間で推移していることが分かる。Safari については 3、4 日目の異常な値が記録されている。システムの影響がでているものと考えられるが、その原因は不明である。

4.2.3 セキュアブレイン分の実験結果の分析・考察

セキュアブレインが収集したフィッシングサイトのURLを用いた実験結果についての分析、考察について述べる。

(a) 検知率：1 日当たりの検知数の平均と、検知率は以下となる。

表 4.2-5　セキュアブレイン分の検知率

(29 件中)	IE7	IE8	Safari	Firefox
検知数	0	0	7.6	7.8
検知率(%)	0.0%	0.0%	26.2%	26.9%

検知率については、Firefox と Safari が約 26%台、IE については 0.0%となっている。

(b) 有効検知率：有効検知数の平均と有効検知率を以下に示す。

表 4.2-6　セキュアブレイン分の有効検知率

（29 件中）	IE7	IE8	Safari	Firefox
有効検知数	14.6	14.8	11.6	14.4
有効検知率(%)	50.3%	51.0%	40.0%	49.7%

有効検知率については、IE8、IE7、Firefox、Safari の順に高くなっている。しかしながら、全般的に 40~50%台と、他のデータに比べて低い値になっており、PhishTank 分や JPCERT/CC 分を用いた場合と比較して、異なる傾向が表れている。

(c) 検知率の推移：検知数の推移の観点からデータの抽出を行った。

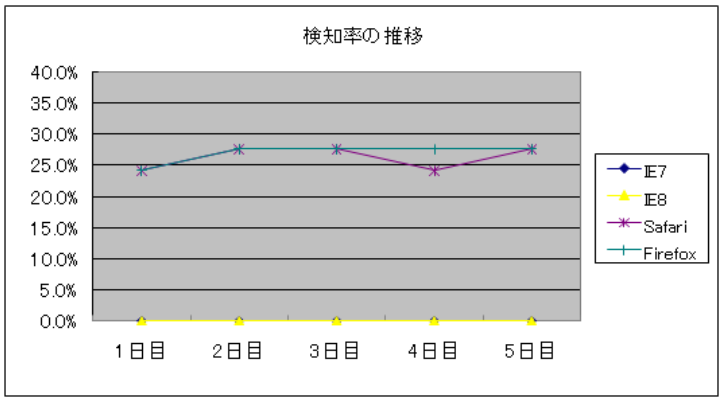

図 4.2-5　セキュアブレイン分の検知率の推移

(d) 有効検知率の推移：有効検知率の推移の観点からデータの抽出を行った。

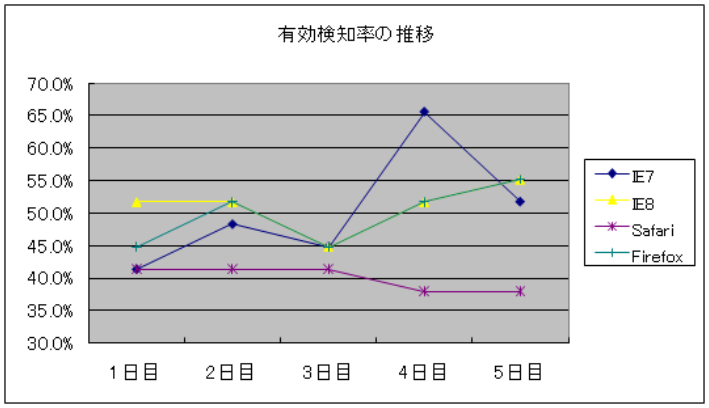

図 4.2-6　セキュアブレイン分の有効検知率の推移

図 4.2-6 に示したグラフをみると、全般的に PhishTank 分や JPCERT/CC 分を用いた実験よりも有効検知率が低くなっている。なお、(a)で示した検知率では IE が 0%となっていたが、有効検知率の観点から見ると、各ブラウザで大きな差はない。

5. まとめ

本調査では､4つのメジャーなブラウザであるInternet Explorer 7,Internet Explorer 8、Firefox 3.5、Safari4 を対象として、これらのブラウザがデフォルトで有しているフィッシング検出機能の有効性や課題について調査を行った。以下、ブラウザ別の検知率、検査データの提供元別の検知率、継続調査を行った場合の検知率の推移について考察する。

5.1 各ブラウザによる検知率

純粋に検知率のみを対象とした場合、3 つの調査対象データのいずれについても、最も検知率が高いブラウザは Firefox であった。ついで Safari、IE8、IE7 の順になることも、共通していた。大きく IE と Firefox および Safari の二つに分かれる理由としては、IE は Microsoft 社の独自のブラックリストや判定アルゴリズムを使用しており､Firefox と Safari は Google 社の Safe Browsing API を使用していることに起因すると推測される。

しかし、検査データはいずれも悪質なフィッシングサイトである、またはかつてそうであった URL のリストであることから、単純に検知率だけを持って有効性を測ることはできない。当該 URL のサイトが生存していれば検知されなければならないが、すでに閉鎖した場合などは未検知ではなく、404/403 を取得できなければならないからである。よって、検知数とコンテンツ未確認数の和から求められる有効検知率の観点から検知率をとらえなおしてみると、やはり Firefox が最も高い値をしめすものの、いずれのブラウザもおおむね同等の有効検知率を示している。このことから、一般のユーザが Web を閲覧する場合においては、どのブラウザを使用してもフィッシングサイトを検知する機能の精度については、それほど大きな差はないと結論付けることができる。ただし、3.1(9)(a)で述べたように、Google 社の Safe Browsing API は、API を利用する実装側の実装方法によって判定結果に差が生じる場合がある。Google 社が提供するのは URL をハッシュ化したリストのみであり、実装者は判定したい URL をハッシュ化した上で、そのリストと対比させなければならない。必ずしも Google 社の意図したとおりにリストが活用されないことを考えれば、評価基準がある程度均一なものになる Internet Explorer の方が高い精度を有していると考えることもできる。

5.2 検査データの提供元による検知率

検知率の順位については､PhishTank 分､JPCERT/CC 分を用いた実験の結果は､Firefox＞Safari＞IE8＞IE7 となり、JPCERT/CC 分のほうが検知率が低いものの、同様の傾向が表れていた。セキュアブレイン分を用いた実験では、いずれのブラウザについても、検知率が他のデータに比べて低く、特に IE については検知数が 0 件であった。これらの結果から、PhishTank 分、JPCERT/CC 分、セキュアブレイン分の順に検知率が低くなることが分かる。

一方、有効検知率について見てみると、PhishTank 分と JPCERT/CC 分では、おおむね80%前後の高い数値を示しているが､セキュアブレイン分については､50%前後の値を示している。

セキュアブレイン分を用いた実験において、他の検査データと比べ検知率が低い理由について考察する。まず、PhishTank 分、JPCERT/CC 分、セキュアブレイン分のそれぞれの出所について整理してみる。PhishTank 分のデータは、米国のコミュニティサイトから収集したものであるが、このデータの中には米国のアンチフィッシング・ワーキング・グループ（APWG）が PhishTank に提供したフィッシングサイトのリストが多数含まれていると予想される。この APWG が PhishTank に提供するリストは、同様に Microsoft 社や

Google 社の他、セキュリティベンダなど、APWG の会員企業にも提供されていると考えられる。このため、PhishTank 分はブラウザのフィッシング検知機能向けに各社が作成するブラックリストと類似性を持っている可能性がある。次に JPCERT/CC 分についてであるが、JPCERT/CC にはフィッシング対策協議会などからフィッシングの URL の報告を受けている。そのため日本国内のブランドを標的とするフィッシングサイトの情報が多く含まれている。これらのフィッシングサイトの情報については、PhishTank のようにデータの収集と整理が行われておらず、ブラウザベンダの提供するブラックリストへの反映が不十分である。このため、JPCERT/CC 分の検知率は、PhishTank 分と比べ、低いものとなったと考えられる。

最後にセキュアブレイン分については、日本国内のユーザが、Web 巡回中、あるいはスパムメールなどで取得し、登録したフィッシングサイトの情報である。一般にはあまり知れ渡っていないフィッシングサイトである可能性はあるが、サンプル数が少ないため、今回の検証では考察を控えたい。

5.3 継続調査を行った場合の検知率の推移

新たなフィッシング URL がブラックリストに登録されるまでに、どの程度の時間を要するか確認するために、同一 URL を 5 日間連続して検証した。結果、いずれのブラウザについても 2 日目に検知される確率がピークとなることが分かった。

また検知結果から、いずれのブラウザについても、生存していないサイトについてはブラックリストから除外しているものと推測されるが、その精度は IE が好成績を残した。

5.4 総括

複数の情報源から入手した 1300 以上の URL を用いて、ブラウザ搭載フィッシング検出機能の検知率を評価した。事前の調査どおり 4 つのブラウザ全てが、ブラックリスト方式を使っていることが確認された。

URL がフィッシングとして検知される率については概ね 8 割から 9 割という、当初の予想を上回る結果が得られた。この結果から、ブラウザ搭載フィッシング検出機能は一定の効果が期待されること、および消費者向けにその使用を促すことの妥当性が認められた。また PhishTank で公開されている URL が、JPCERT/CC に報告されるものよりも検知率が高いという傾向が確認された。

一方でブラウザ搭載フィッシング検出機能の検出精度の限界もみえてきた。検知率は 8 割から 9 割であると述べたが、5 日の調査期間中の初日にはより低い検知率であった。PhishTank などのデータベースからブラウザが持つ URL ブラックリストへの反映には最大で約 24 時間を要することが確認されており、ブラックリストへのデータ反映の即時性には今後改善の余地が残されていると考える。

フィッシング対策協議会は 2010 年 2 月から会員/オブザーバーの中でフィッシング対策ツールバーなどの製品を持っている企業に対して URL 提供の取り組みを始めた。このような取り組みを拡大し、メジャーブラウザベンダや大手セキュリティソフトベンダとの連携を強化することは消費者保護の観点から推進すべき課題の 1 つと考えられる。その際に、本調査で明らかとなった課題や、フィッシング URL の増加や即時性の高さに配慮したスキームを構築していくことが望まれる。