フィッシングに関する国際調査報告書

2013 年上半期の傾向とドメイン名利用

Anti-Phishing Working Group

(フィッシング対策実務者グループ)

発行 2013 年 9 月 18 日

著者

ロッド・ラムンセン：インターネットアイデンティティ社

グレッグ・アーロン:イルミンテル社

研究、分析補助及び画像提供

アーロン・ロット:インターネットアイデンティティティ社

目次

お断り： 本報告書は、APWG、APWG共同調査員、研究員、およびベンダにより、専門家の知識、意見を元に「公共に資する為に」作成された。そのため、調査データの完全性、正確性、および関連性について、並びに企業運営に関する、或いは攻撃手法の対策に関する勧告について我々は保証できないことをご了承いただきたい。本報告書には著者の研究および意見が含まれている。詳しくはAPWGのウェブサイト(apwg.org)を参照いただきたい。

概　　要

フィッシング詐欺者は常に存在を知られぬよう影に紛れている必要があるが、フィッシング攻撃による成果を見るためには犠牲者が必要となる。フィッシングの手法は刻一刻と変化しており、フィッシングに対抗するためにはフィッシング詐欺者が如何様にして偽サイトを作成し、広めているのか学ばなければならない。我々は、2013年上半期に発生したフィッシング行為を分析することで、彼らの攻撃手段を突き止めた。悪意ある詐欺者は新しい手法を試み、新しいリソースを利用している。善意のフィッシング詐欺者は一部のハッカー大会に出場し・勝利している。全体的に、インターネット利用者数が増加している地域においてフィッシングが拡大している。

本報告書は、世界中で起きているフィッシング問題を数値化し、フィッシングの傾向と重要性を把握することを目的に作成された。そのため、我々は報告書作成にあたり2013年上半期(1月1日～6月30日)に検知された全てのフィッシング攻撃を精査した。調査データはAPWG(Anti-Phishing Working Group、以下APWGとする)が収集したものに加え、フィッシングに関するフィード、CNNIC(中国ネットワークインフォメーションセンター)および民間の情報源によりデータの補強がなされた。APWGフィッシングデータベースはインターネットにおける最も包括的なフィッシング、およびメール詐欺を記録するアーカイブである。データを共有していただいたCNNICおよび中国フィッシング対策連盟(the Anti-phishing Alliance of China、APAC)には感謝の意を厚く表したい。

本報告書の摘要を次に示す。

1. 脆弱なホスティング業者が意図せずフィッシングの一因となっており、脆弱なホスティング業者を利用したフィッシング攻撃が全体の27%を占めた。(8~9ページ)

2. 増えゆく中流層がより一層電子商取引を利用するようになった中国において、依然としてフィッシングが拡大を続けている。(12、および14~15ページ)

3. フィッシングで狙われる標的(ブランド)の数が上昇した。これによりインターネット犯罪者が時間をかけて攻撃の機会を伺っていることがわかった。(6ページ)

4.ひと目の付かない小規模なドメイン名登録団体(レジストラ)、登録管理団体(レジストリ)およびドメイン取得代行業者(リセラ)が引き続きフィッシングに利用されている。今後二年でTLDのレジストリの数が5倍になる勢いとなっている。**(9~12および16~17ページ)**

5. フィッシング攻撃の平均及び中央稼働時間(平均値・中央値)が上昇している。(6~7 ページ)

主な統計結果

2013 年上半期に何百万件ものフィッシングサイトが報告されたのに対し、固有のフィッシング攻撃およびフィッシングサイトをホストするドメイン名の報告件数は少なかった[1]。2013 年上半期の調査データにより、以下の統計結果が得られた。

- **全世界で少なくとも72,758件の固有のフィッシング攻撃が発生した。**この数字は、2012年下半期の記録である123,486件と比較すると遥かに低い数値である。一度に複数のドメインに侵入できる仮想共有サーバーを利用したフィッシング攻撃が減少したためだ。(8ページ「仮想共有サーバーへのハッキング」を参照)。**本書では「攻撃」には「特定のブランド(或いは組織)を標的にしたフィッシングサイト」が含まれている。**

  例:単一のドメイン名は異なる複数の銀行に対し、個別にフィッシング攻撃(詐欺サイト)をホストできる。
- **固有のドメイン名[2]において53,685件の攻撃が発生した。**この数値も2012年下半期の記録である89,748件と比較すると減少している。こちらの原因としては、仮想サーバーへのハッキング報告件数が減少したことがあげられる。全世界におけるドメイン名の数は、2012年11月の258万個から2013年4月で261万個に増加した[3]。
- **また、ドメイン名を使用せず、1,626個の固有なIPアドレス上で1,972件の攻撃が検知された。**(例: http://142.234.140.62/pay/jian)。IPアドレスを利用した攻撃の件数は3年半、横這いとなっている。なお、IPv6アドレス上ではこのような攻撃は報告されていない。
- フィッシングに使われた53,685個のドメイン名の内、**12,173個がフィッシング詐欺者によって悪意をもって登録されたものであると特定した。この数字は2012年下半期に発見された5,835件のおよそ2倍である。増加の原因として、中国系フィッシング詐欺者によるドメイン登録が突如増えたことがあげられる。**その他41,532個のほぼ全ては、脆弱なウェブホスティングサーバー上でハッキング若しくは不正な侵入により登録されていた。
- **フィッシング攻撃の平均稼働時間が2012年初頭の歴史的に低い値から上昇している。2012年下半期における平均稼働時間の26時間13分に対し、2013年上半期における平均稼働時間は44時間39分だった。**

---

1 これにはいくつか要因がある。
(A) 一部のフィッシングでは、URL に固有の数字を組み込むことでしばしば標的を追跡したり、スパムフィルターをすり抜けたりするなどのカスタマイズされた攻撃が行われているため。それ故、ひとつのフィッシング攻撃で何千もの URL が報告されるが、本質的にはその攻撃はひとつのドメイン名上で行われている。その結果、全ての URL を数えたことで、フィッシング攻撃の検知数が大きくなる場合がある。固有な攻撃を計数するために、我々の計数方法では重複を避けるようになっており、これは過去の報告書においても同様である
(B)フィッシング詐欺者はひとつのドメイン名を用いて、異なる標的に同時に攻撃をしかけることが多いため。つまり、一部のフィッシング詐欺者は自身が登録したドメイン名上に複数の異なるフィッシングサイトを設置しているためだ。
(C)フィッシングサイトが複数のページで構成されていてその銘々が報告されている可能性があるため

2 「ドメイン名」とは第 2 レベルドメインにおけるドメイン名のことを指す。加えて、第 3 レベルドメインのものも、レジストリが登録を受け付けている場合は含まれる。例えば、 .CN を受け持つレジストリでは第 2 及び第 3 レベルドメイン(com.cn、 gov.cn、zj.cn ゾーン下などにおいて)の登録を受け付けている。TLD 下におけるフィッシング活動の報告件数が減少したことについては、「サブドメインを利用したフィッシング攻撃」の項目を参照しいただきたい。

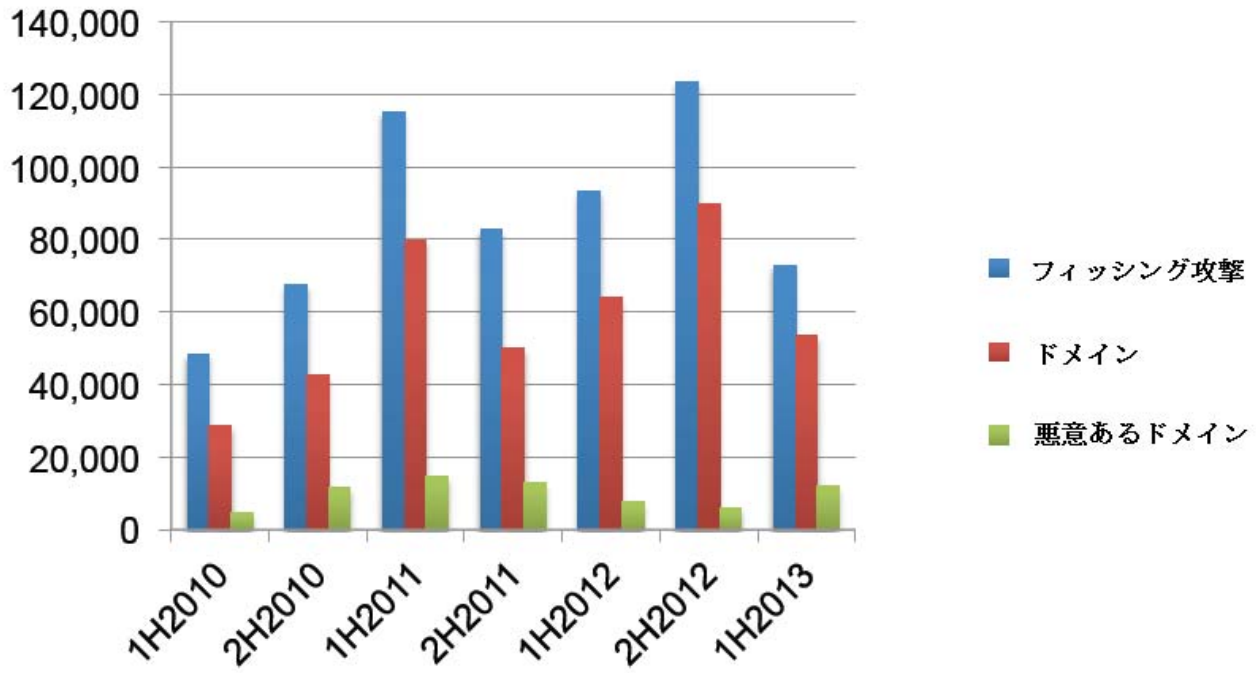
3 この数値はICANN.orgが提供するgTLDの統計データ、ccTLDレジストリの運営団体が提供する統計データも含まれている。

2013年上半期における稼働時間の中央値は12時間52分で、歴史的に見て低い値であった2012年上半期における中央値、5時間45分の二倍以上であった。

- **195のトップレベルドメイン(TLD)でフィッシングが発生したものの、悪意あるドメイン登録の82%はわずか３つのTLD下で行われた。即ち、.COM、.TK、そして.INFOの３つである。**
- **720の団体・組織が標的にされた。2012年下半期に特定した611団体から比較すると上昇が顕著である。**
- **フィッシングに使われた全てのドメイン名の内、その名前にブランド名、若しくはそれに準じる表現が含まれていたのはわずか2.3パーセントであった。**(以下の「危険なドメインVS悪意ある登録」を参照)
- 攻撃が発生したドメイン名53,685個の内、78個は国際化ドメイン名で、更に78個中3個は同形異義語(ドメイン名を偽装する)攻撃に利用された。
- URL短縮サービスを悪用したフィッシングの件数が急落した。URL短縮サービスを提供する団体がより強力な悪用防止策を実施したことによるものと思われる。

統計データ

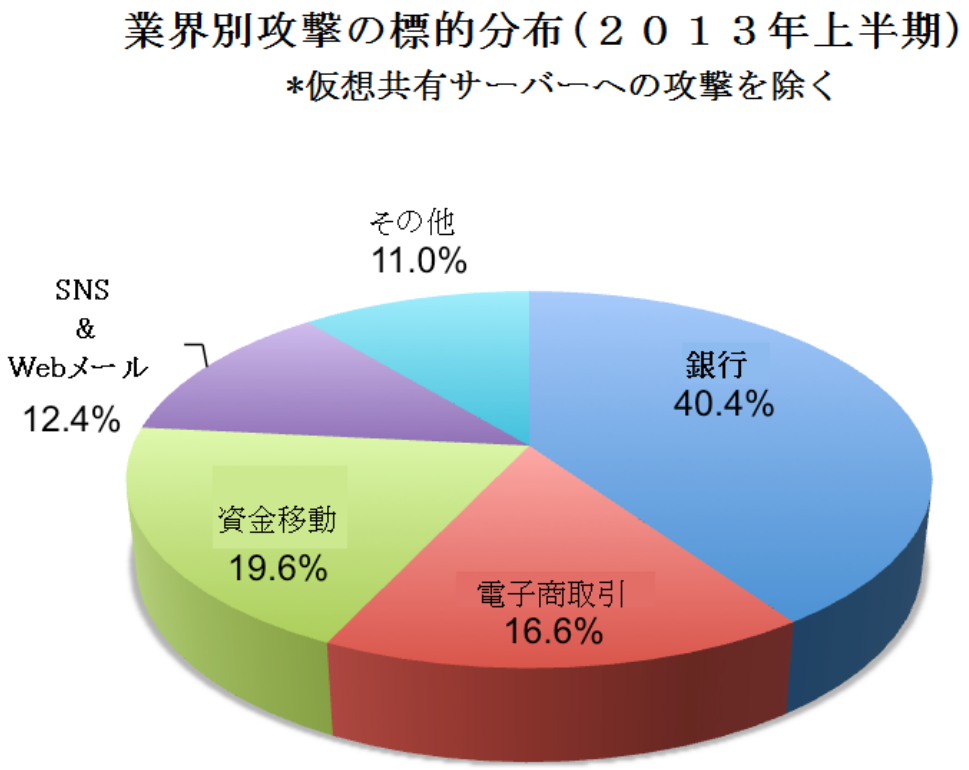
	2013 年 上半期	2012 年 下半期	2012 年 上半期	2011 年 下半期	2011 年 上半期	2010 年 下半期
フィッシングドメイン名	53,685	89,748	64,204	50,298	79,753	42,624
攻撃件数	72,758	123,476	93,462	83,083	115,472	67,677
利用された TLD 数	194	207	202	200	200	183
IP によるフィッシングの件数(固有 IP 数)	1,626	1,981	1,864	1,681	2,385	2,318
登録された悪意あるドメイン数	12,153	5,833	7,712	12,895	14,650	11,769
IDN ドメイン数	78	147	58	36	33	10
標的の数	720	611	486	487	520	587



標的にされた団体・組織の分布

調査期間中、720の団体・組織がフィッシングの標的にされていたことがわかった。2012年下半期に特定した611団体から比較すると上昇が顕著である。標的にされた団体・組織は長期に渡り攻撃の被害にあっている。

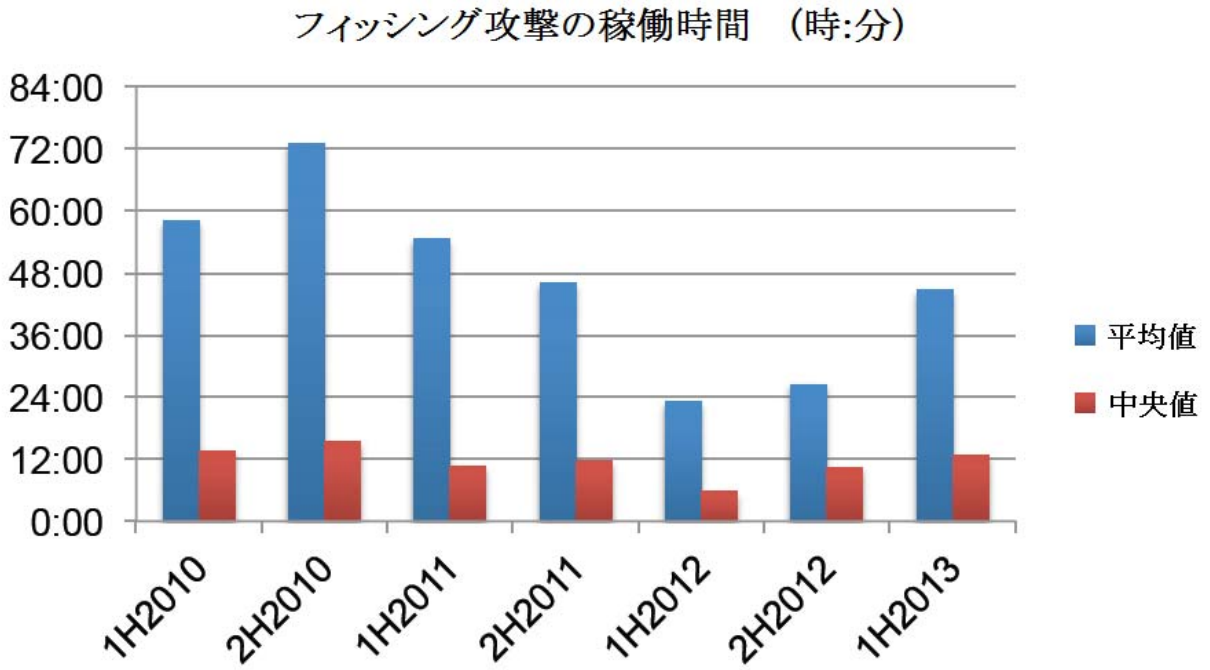
- 最も標的にされた回数が多かった団体・組織は、PayPalで(13,498回、全体の18.3パーセント)、2番目に多かったのがTaobao.comだった(6,605回、全体の9%)。
- 標的にされた回数が多かった上位80の団体は期間中に100回以上の攻撃を受けた。
- 半数は期間中に１～３回の攻撃を受けた。



稼働時間からみたフィッシング

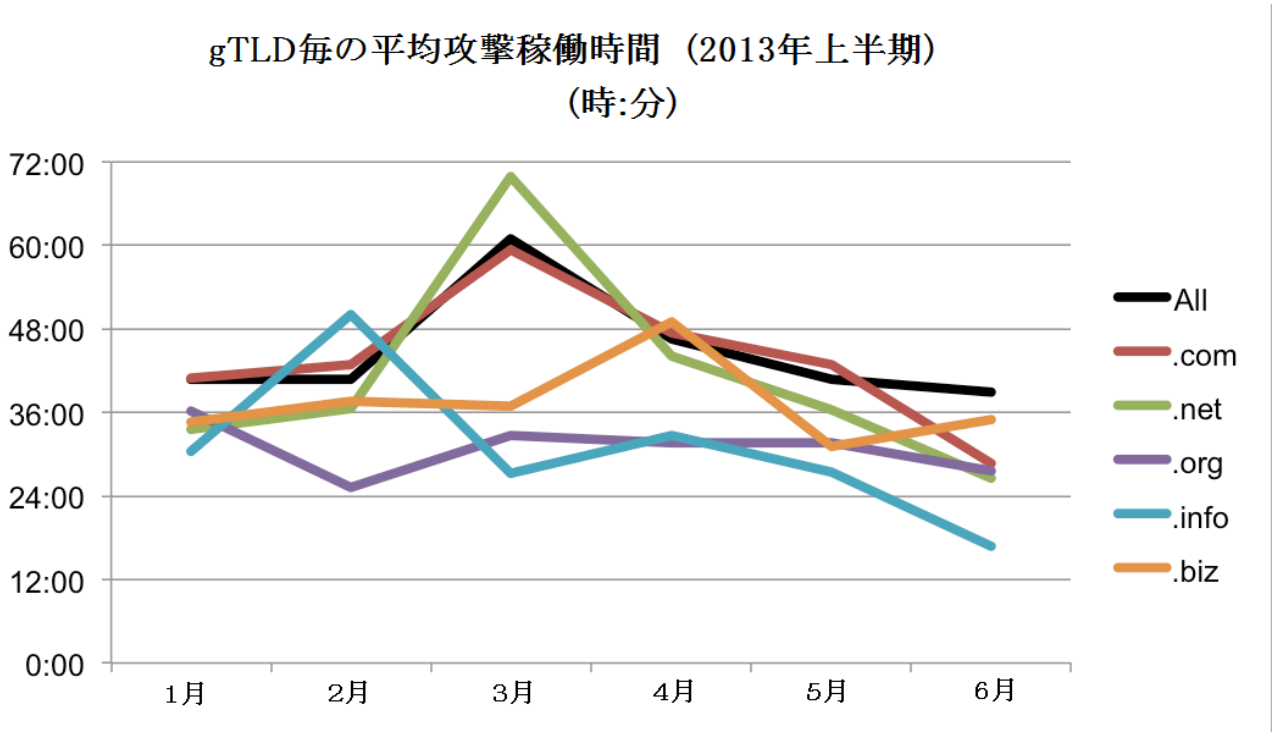
フィッシング攻撃の平均稼働時間が2012年初頭の歴史的に低い値から上昇している。2012年下半期における平均稼働時間である26時間13分に対し、2013年上半期における平均稼働時間は44時間39分だった。2013年上半期における稼働時間の中央値は12時間52分で、歴史的に低い値であった2012年上半期における中央値5時間45分の二倍以上であった。

フィッシング攻撃の「稼働時間」、即ち「生存時間[4]」はフィッシング攻撃の影響を計るのに欠かせない要素だけではなく、対応の効果を見る手段でもある。フィッシング詐欺者にとっては、攻撃初日が最も有益であるため、可及的速やかな対応が必須となる。数週間、数カ月と残り続ける一部のフィッシングサイトによって稼働時間の平均値が押し上げられるため、中央値もまた対応策の効果を見る際の有用なバロメーターとなる。CNNICが検知したフィッシングの稼働時間については記録されていないため、本統計の稼働時間の算出には含まれていない。

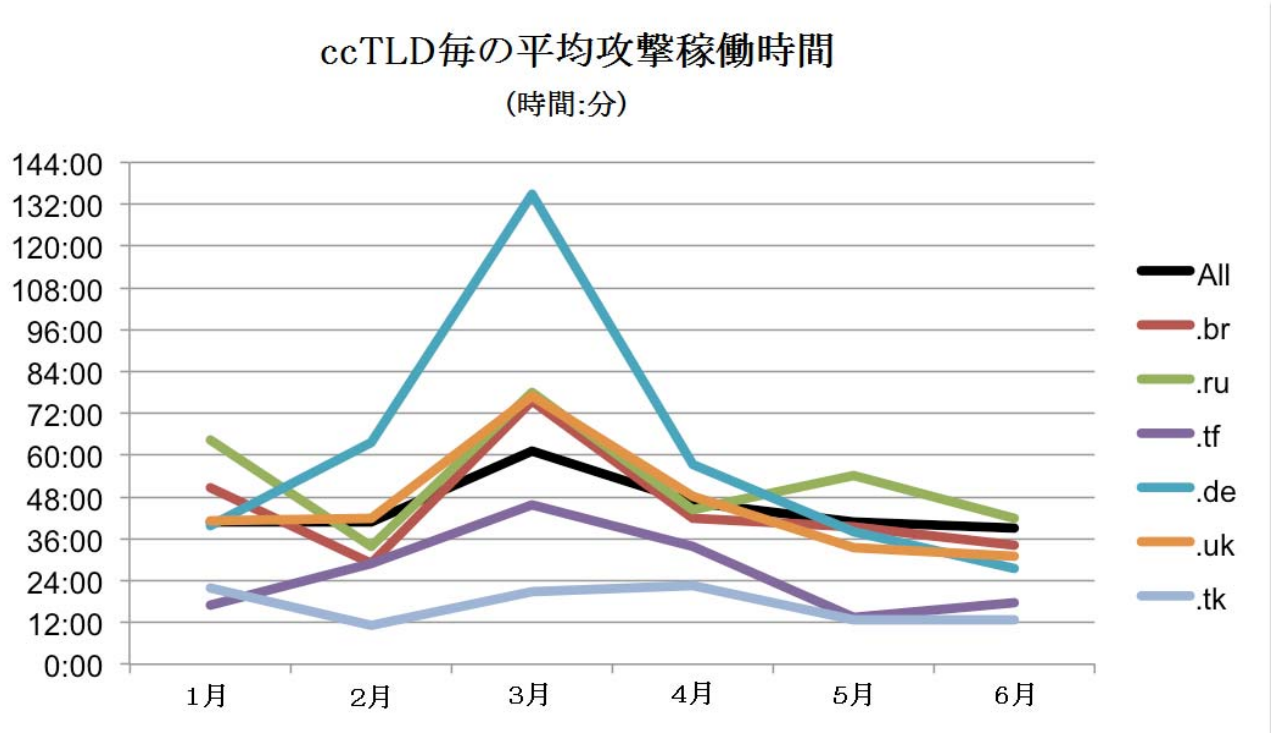


登録数の多い分野別TLD(以下gTLD)において、3月では仮想サーバーへのハッキングが減る一方でフィッシング攻撃の稼働時間が伸び、逆に4月には仮想サーバーへのハッキングが増えるにつれ、攻撃の稼働時間が短縮した。(仮想サーバーへの攻撃により、被害にあったホスティング業者に対し大量の通知が一度に送信され、ハッキングされたサーバーが明らかになる。そのため、各々の対応策で同時に複数のフィッシング攻撃を駆除できる。)。.INFO、.BIZ、そして.ORGにおける稼働時間は引き続き平均以下を保っている。これらのレジストリ運用側に攻撃通知・駆除プログラムがあるためだ。

[4] 稼働時間を自動的に記録するシステムにより、フィッシングサイトを監視した。システムはフィードやハニーポットによってフィッシングを検知すると、即座に監視を開始する。フィッシングサイトを一時間に数回チェックすることで稼働状態を確認し、サイトが最低でも一時間閉鎖されていなければ「閉鎖された(down)」と判断しない。(これは、一部のフィッシングサイト、特にボットネット上にホストされているサイトは、毎回名前解決されるわけではないが通常そのまま生存しているためである)。10 パーセント以上のフィッシングサイトが閉鎖されて一時間後に「復活」することがあるため、各フィッシングサイトの「正味の」稼働時間はより少なく計測されている可能性がある。しかし、我々の調査手法ではインシデント間での直接比較や相対比較が可能であり、測定方法としては一貫性がある。



登録数の多い国別TLD(以下、ccTLD)によって、稼働時間にはばらつきがあった。



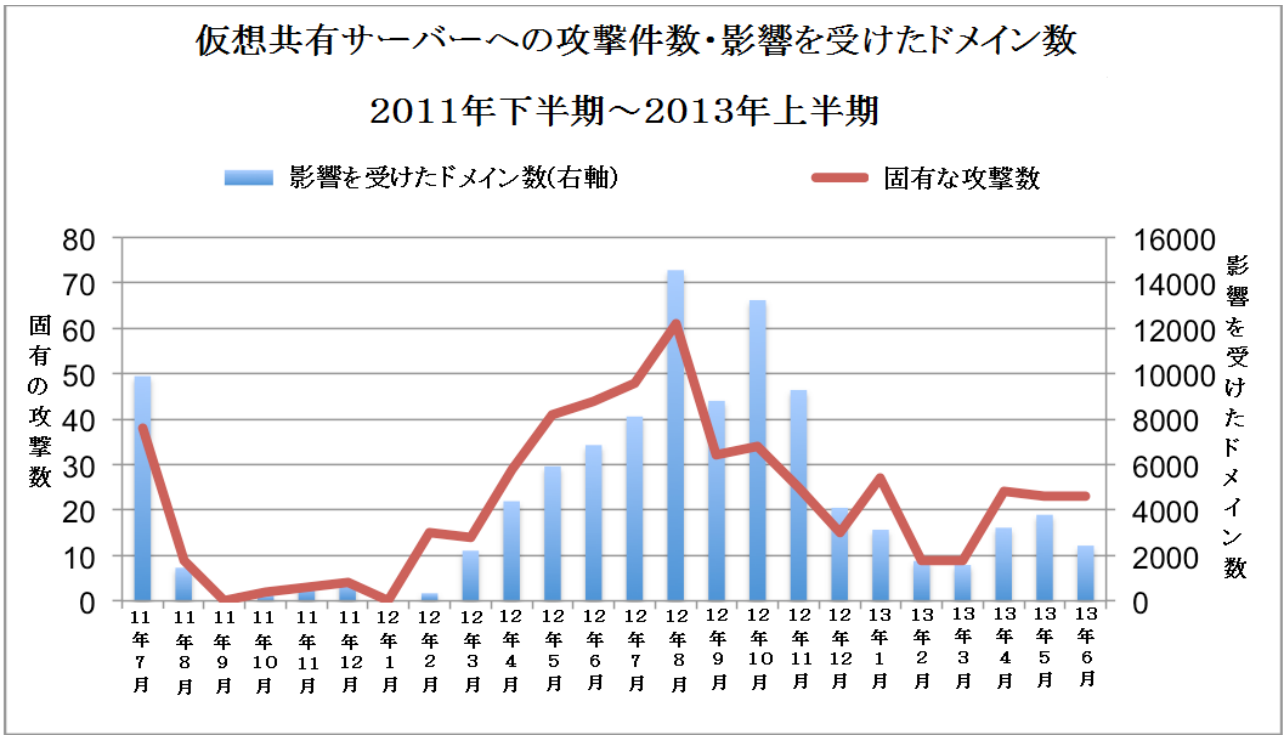
全てのTLD下における攻撃稼働時間については本報告書末尾の付録をご覧いただきたい。

仮想共有サーバーへのハッキング

仮想共有サーバへのハッキングについては、とある攻撃方法が我々の統計に深く影響を与え続けている。その攻撃ではまず、フィッシング詐欺者は数多くのドメインをホストするウェブサーバー、つまり仮想共有サーバーへ侵入する。そこで彼らはフィッシング用に作ったコンテンツのコピーをアップロードする。次にサーバーの設定を変更し、そのコンテンツをそのサーバーが管理するすべてのホスト名に追加する。こうすることでサーバー上の全てのウェブサイトはフィッシングのページを表示してしまう。複数のサイトをひとつひとつハッキングするのではなく、フィッシング詐欺者は、サーバーによっては一度に何百ものウェブサイトをハッキングする場合がよくある。

2013年上半期において、こうした類の大規模なサーバーへの侵入が115件あったことがわかった。これにより19,455件のフィッシング攻撃が発生した。

これは世界で記録された全フィッシング攻撃の27パーセントを占めるものであるが、2011年下半期の58,100件からは減少している。



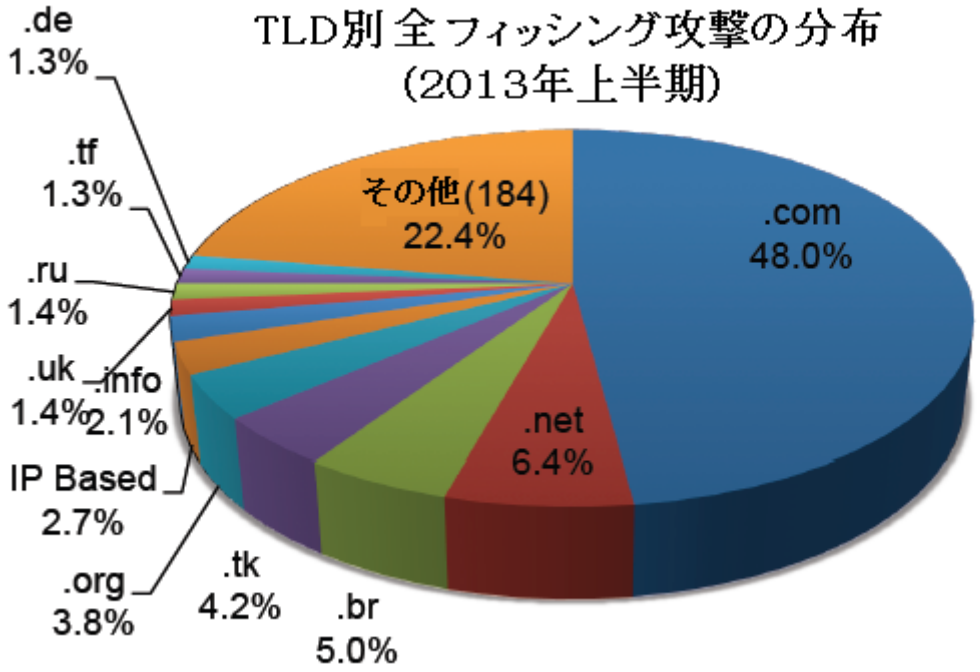
我々は、攻撃に使われた端末のIPアドレスや、攻撃のタイミングを分析し、そしてフィッシング詐欺者の共

有し且つ露見しているURLパスから攻撃方法を特定した。
ホスティングサーバーに侵入することは詐欺者にとって高効率なアクティビティであり、彼らはホスティング施設にある脆弱なサーバーを利用する傾向がある。ホスティング施設では沢山の高性能サーバーや、大量のトラフィックを転送できる大規模な「パイプ」と呼ばれるものが収容されており、これらを組み合わせることによってホスティング業者は家庭用パソコンよりも遥かに高い演算処理能力や広い帯域幅を実現している。

我々は、共有ホスティング環境を標的にするために使われることの多いツールや特にWordPress, cPanel, Joomlaのインストール状況を継続して監視していく。自動クラッキングツールにより、データセンターの新しいサーバーが様々な市場を介して犯罪の温床にされてしまっている。我々は斯様なサーバーが、フィッシングに留まらず、闇に潜むプロキシネットワークからBrobotやDNS増幅攻撃による大規模なDDoS攻撃に至るまであらゆる方面に利用されているのを観測してきた。この問題については、ウェブホスティング業者同士のコミュニティそしてウェブセキュリティのコミュニティが協働で改善に努める必要があるが、ホスティング事業は利ざやが少なく、リセラが何層にも連なっており、そしてホスティング業者には悪用対応能力が殆ど若しくは全くないことが多い。その為、来年においては業界として非常に難しい課題に取り組むことになる。

TLD からみたフィッシングの流行度

フィッシングに使われたドメインや、フィッシング攻撃を分析し、TLD間におけるフィッシングの分布を調べた結果、相変わらずフィッシングの大多数は僅か数種の名前空間に集中していることがわかった。ほとんどのフィッシングは脆弱なドメイン名上で行われていて、TLD毎の分布はTLDの市場占有率とおおよそ同じとなっている。



TLDにおけるフィッシングの流行度を計るために、我々は「ドメイン10,000個あたりのフィッシングドメイン」と「ドメイン10,000個あたりのフィッシング攻撃」という二つの尺度を採用した。「10,000個あたりのフィッシングドメイン[5]」とは、１つのTLD下で登録されているドメイン名の数に対する、フィッシングに使われたドメイン名の数の割合をスコアとして算出したもののことである。この尺度により、TLD間のフィッシングの発生率の高低を明らかにすることができる。

「ドメイン10,000個あたりのフィッシング攻撃」という尺度もまた、名前空間におけるフィッシングの流行度を計る有用な手段である。とりわけ、この尺度ではサブドメインを利用しているフィッシング詐欺者がどのTLDを優先的に使用しているか、どのドメインに複数のフィッシングサイトが開設されているかを明らかにできる。

上記の尺度による数値を含む全TLDの調査データ一覧は報告書末尾の付録にて示す。

5 計算方法(スコア)=(フィッシングドメインの数÷TLD 下にあるドメインの数)×10,000

• **ドメイン10,000個あたりのフィッシングドメインのスコア中央値は3.1だった**(2012年下半期は4.7).

• **最も使用量の高い.COMのドメイン10,000個あたりのフィッシングドメインのスコアは2.5だった。**本調査データ内の全フィッシングドメインの内52パーセント、そして世界中で使われているドメインの42パーセントが.COM下に置かれていた。

したがって、ドメイン10,000個あたりのフィッシングドメインのスコアは2.5~3.1が「中程度」と推察する。3.1以上のスコアであるTLDは、そのTLD下でフィッシングが広く流行していると判断した。[6]

スコアからみた上位のTLDは以下の通り。

フィッシングドメインのスコアが高いTLD(2013年上半期)

最低 25個のフィッシングドメインおよびレジストリ内には最低 30,000 個のドメイン

順位	TLD名	TLD地域	固有の攻撃の報告件数(2013年上半期)	フィッシングに使われた固有なドメイン名数(2013年上半期)	レジストリ内のドメイン数(2013年4月時点)	ドメイン10,000個あたりのフィッシングドメイン数(2013上半期)
1	.pw	パラオ	115	109	55,000	19.8
2	.np	ネパール	97	64	32,500	19.7
3	.th	タイ	166	125	65,350	19.1
4	.si	スロベニア	219	196	108,100	18.1
5	.ec	エクアドル	64	48	30,500	15.7
6	.pe	ペルー	143	107	69,505	15.4
7	.sa	サウジアラビア	40	33	30,400	10.9
8	.cl	チリ	494	357	418,558	8.5
9	.br	ブラジル	3,668	2,669	3,265,768	8.2
10	.ma	モロッコ	44	33	43,299	7.6

[6] 本統計に関する注意点:
- 使用量の低い TLD では、少数のフィッシングドメインでスコアが大幅に増加する可能性があり、これにより中央値が押し上げられている。TLD の規模が大きいほど、一つのフィッシングドメインによるスコアの影響は小さい。
- レジストリのスコアは、頻繁に攻撃を行う一人のフィッシング詐欺者や一つの脆弱な小規模レジストラの些細な行動で増加する可能性がある。
- TLD のスコアに影響を与える要因や背景については、過去の調査にある “Factors Affecting Phishing Scores”を参照いただきたい。

.PWはパラオ国のccTLDであるが、2013年3月25日に「Professional Web」を意味するgTLDとして登録が再開された。フィッシング詐欺者やスパムメール送信者がこのドメイン空間で実験的にフィッシングやスパム行為を行った結果、レピュテーションサービス業者によってネットワークのブロックや、禁止リストへの登録が行われた。そのため、こうした新しいgTLDには悪用を防ぐための監視を適切に実行する必要がある。この問題に対抗するため、.PWのレジストリ運営者により、さらなる悪用防止策が実施された。その結果、悪用の検知件数が急激に減少した。

タイのccTLDである.THは政府や大学の脆弱なWebサーバーが主な原因となり、長らく上位にランクインし続けている。第９位の.BR下の脆弱なドメイン名において、世界中で南米銀行を含む171の団体がフィッシングの被害にあった。

インターネット上のTLDを統括している団体であるICANNの主導による複数年計画および適用プロセスの結果、2013年下半期から2015年にかけて、およそ1,200個の新しいTLDが追加される予定だ。一般企業が管理する一部の新しいTLDはそれらの企業内のみでの使用に「限定」されることになり、これによって悪意あるドメイン登録を防ぐことができる。また、指定したコミュニティにおいてのみ使われる新しいTLDもある。こうした制限付きの登録方針によってフィッシングを防げる可能性がある。多くの新しいTLDは一般に開放され、世界中の人々が登録を行うことができるが、同時にフィッシング詐欺者に絶好の機会を与えてしまうことになる。

ドメインの悪用を取り締まり、ブランドの所有者を保護するために、様々な対策が新しいTLDにおいて実施されている。例えば効率的で新しい調停手続きを導入したり、トレードマークを所有する人々向けにドメイン名優先登録期間を設けたり、そしてレジストラに対して悪用の報告を受け付ける窓口の設置を義務付けたりしている。ICANN公認レジストラでは、WHOISレコードの正確性向上及びフィッシング詐欺者によるWHOISレコード内の偽情報の挿入を防ぐことを目的に新しいドメイン登録者確認手続きを開始した。しかし、フィッシング詐欺者から新しいTLDを保護するためには、システムだけでなく人による監視も必要である。我々は新しいTLDの導入を慎重に見守り、重要なイベントを報告していく。

脆弱なドメイン VS 悪意あるドメイン登録

我々は、脆弱な（ハッキングされた）ドメイン上に存在するフィッシングサイトに対してどれだけ多くのドメイン名がフィッシング詐欺者によって登録されたのか調査した。これは、対応策を行うべき者が特定できたり、フィッシング詐欺者がどのようにしてフィッシングを行っているか把握できるため重要である。以下の条件のいずれか、若しくは全てに当てはまるドメインを悪意あるドメインとした。
一、登録して間もなくフィッシング攻撃の報告を受けている。
二、ドメイン名にブランド名またはそれと誤解させるような文字列が含まれている。
三、バッチ処理若しくは共通の意図や登録者であると見てとれるパターンで登録されている。

フィッシングに使われた53,685個のドメイン名の内、**12,173個がフィッシング詐欺者によって悪意を以って登録されたものであると特定した。この数字は2012年下半期に発見された5,835個のおよそ二倍である。増加の原因として、中国系フィッシング詐欺者によるドメイン登録が急激に増えたことがあげられる。**その他41,532個のほぼ全ては、脆弱なウェブホスティングサーバー上でハッキング若しくは不正な侵入により登録されていた。

12,173個中、少なくとも8,240個(68パーセント)は、中国にあり、主に中国の顧客に対してサービスを提供しているサイトや業者を標的にフィッシングを行うために登録されたドメイン名だった。[7]他国のフィッシング詐欺者と比較すると、中国系フィッシング詐欺者はハッキングされたドメインや脆弱なWebサーバーを悪用するよりも、悪意あるドメイン登録を行うことによりフィッシングを行う傾向がある。2013年上半期のドメイン登録状況を見ると、中国系フィッシング詐欺者はますますリソースに対して貪欲になりつつある。主にTaoao.comや中国工商銀行(ICBC)、CCTV,ZJSTV,そしてTencentが標的にされていた。これらのドメインは主に中国のレジストラにより登録されていたが、アメリカのレジストラによっても登録されており、また中国、アメリカ以外の地域にもホストされていた。より容易に登録が可能なTLDである.TKや.COM,.INFOそして.USが好まれるにも関わらず、中国系フィッシング詐欺者はわずか122個のCN下にあるドメイン名を利用して攻撃を行っていた。

更には、彼らは国外の標的、主にゲームサイトであるBattle.net, Runescape, そしてWorld of Warcraftに対して攻撃を行うために少なくとも450個のドメイン名を追加で登録していた。

中国国外にあるフィッシング観測装置は、CNNICおよびAPACが中国国内で検知したフィッシングのほとんどを検知することができなかった。これは、恐らく観測装置が中国語で書かれたEメールを効率的に解析でき

[7] こうしたフィッシング攻撃は主に中国語で書かれたおとりメールによって広められていた。他の要因についても中国に存在するフィッシング詐欺者を指し示していた。

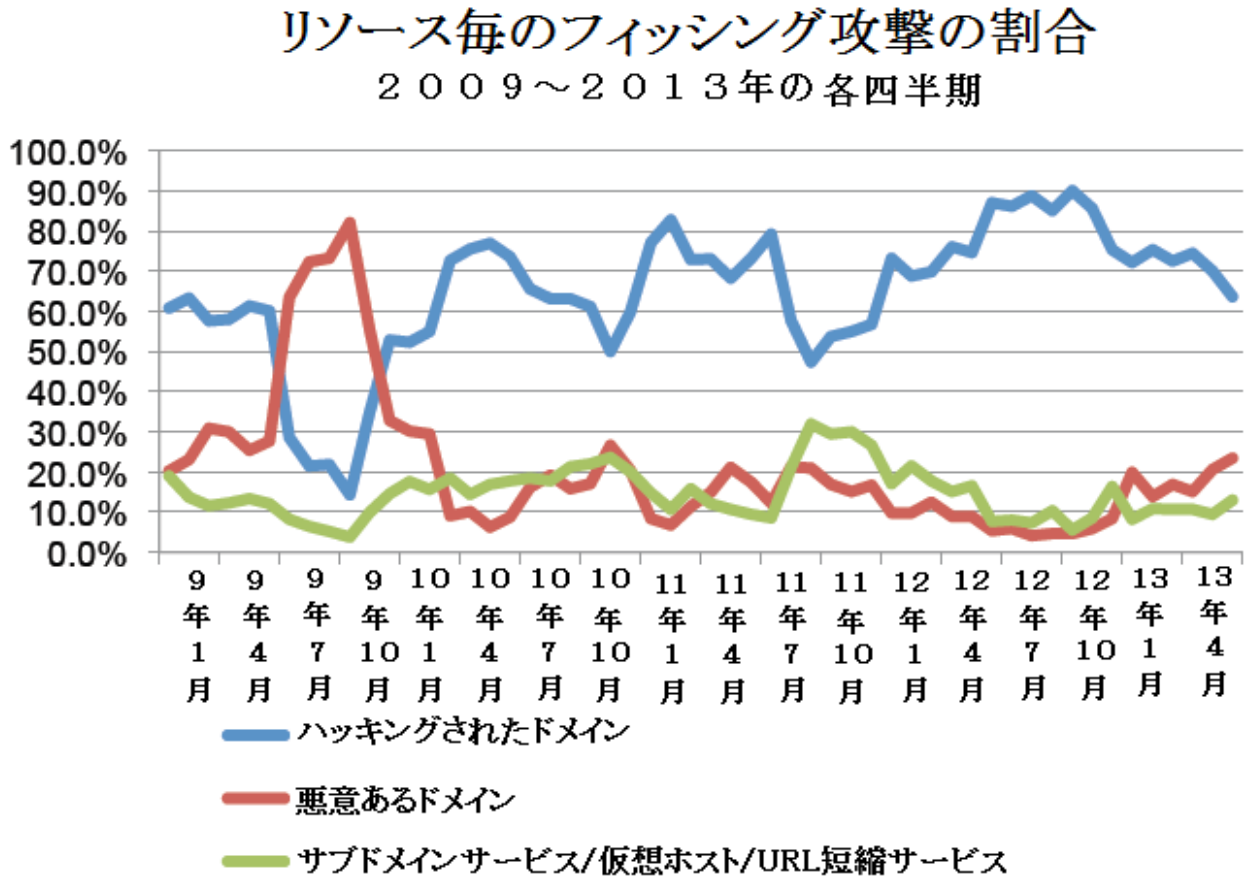
なかったか、若しくは中国国内にハニーポットの設置を依頼できる充分な中国人顧客がいなかったためだろう。いずれにせよ、様々な国々のドメイン登録業者、ホスティング業者、決済インフラが利用され、フィッシング詐欺者だけが利益を得てしまっている。

12,173件の悪意あるドメイン登録の内、およそ82パーセントはたった3つのTLD、.COM (6,477件), .TK (2,801件), and .INFO (655件)の下で行われていた。.COMドメインのレジストリには悪用防止プログラムがなく、.TKドメインのレジストリでは無料でドメイン登録を行うことができ、また認可済みの仲介人に対してレジストリにある.TKドメインの有効期限を直接延長できる権限を与えている。(仲介人にはFacebook, Internet IdentityそしてAPACが含まれている。) 悪意ある登録の頻度は落ちているものの、フィッシングの発生を防ぐには至っていない。.INFOのレジストリを運営する団体には悪用防止プログラムがあるが、他のTLDと比較すると安価にドメイン登録を行うことができ、ドメイン悪用の呼び水の一因となっている。

12,173個中1,244個の悪意あるドメイン名にはブランド名に関連するもの、若しくは類似するもの(多くは綴り違い[8])が含まれていた。これは2012年下半期に発見した数値と同じであった。**この数値はフィッシングに使われた全ドメイン名のわずか2.3パーセント、そして調査期間中に記録された全ての悪意あるドメイン名の10パーセントに当たる。**中国系フィッシング詐欺者が登録したドメイン名の多くは意味のない文字の羅列で構成されていた。

故に、悪意あるドメイン名によってユーザーが惑わされるということは殆ど無く、またドメイン名にブランド名やそれに類似した名前を含めることは攻撃者にとって良策ではない。というのも、ブランド所有者はインターネット上のブランド名に関連するファイルについて積極的にスキャニングを行っているためだ。過去の観測結果の通り、**ドメイン名自体はフィシング詐欺者にとっては重要ではなく、TLD下においてあまり意味のない、若しくは全く意味がない文字列のドメイン名こそが重要である。彼らはブランド名をドメイン名に含めるのではなく、サブドメインやサブディレクトリに含めることが多い。**URL内のどこかに紛らわしい文字列を含ませることで、ユーザーがその部分を見て、騙されてしまう可能性がある。また、URL中の元々の、或いは本当のドメイン名を見分ける十分な力がほとんどのインターネットユーザーにはない。更にはブランド所有者や正当なマーケティングメール送信者は自らの販促のためにトラッキングドメインや、格安のドメインを利用しているが、これらのドメイン名はブランド名若しくは関連商品の名称とは非常にかけ離れた名前になっており、これもまたフィッシング詐欺者を惹きつける呼び水となってしまっている。とどのつまり、ユーザーをフィッシングする時に彼らにとってドメイン名は大した問題ではないのである。

8 調査で見つかったブランド名が含まれたドメイン名の例として、bid-pagzyahoo.com(Yahoo!)や battleuswow.net (World of Warcraft)、ntwestsc.com(NatWest)、そして fbphonenumbers.tk(Facebook)がある。



悪意あるドメイン登録に利用されるレジストラ

フィッシング詐欺者(特に中国系)は2013年上半期において非常に多くのドメイン名を登録していた。彼らは何処でドメイン登録を行っているのだろうか。我々は、gTLDおよびccTLD 下にある12,173個の悪意あるドメイン中95パーセントにあたる11,514個の登録を幇助したレジストラ名を知ることができた。この調査はDomainTools.comによってキャプチャされたWHOISデータによって可能となった。本調査にあたってDomainToolsには御礼を申し上げたい。それらレジストラの管理下にあるドメイン数についてはICANNやその他のリソースを精査し、纏めた。

2013年上半期において、フィッシング詐欺者は少なくとも267のレジストラを利用していた(2012年下半期では少なくとも127以上)。レジストラ市場は多種多様だ。大手レジストラの一角であるGoDaddyはgTLDの市場のおよそ半分のシェアを握っているが、GoDaddyにおいて行われた悪意あるドメイン登録は全体のわずか8パーセントであった。一部のレジストラではリセラープログラムに対応しており、悪意あるドメインの多くはリセラを通して登録・販売されていた。しかしながらリセラの情報はWHOISレコード内には記されないた

め、レジストラの運営者はリセラの身元情報を確認することができなかった。

異なるレジストラを相互に比較するため、我々は様々なTLDを比較する際に用いたものと同様の尺度(レジストラの管理下にある10,000ドメインあたりの悪意あるドメイン)を採用した。この尺度により、レジストラの規模に見合わず頻繁に悪用されているレジストラを特定することができる。下の表の15のレジストラが、全体の66パーセントに当たる8,059件の悪意あるドメイン登録に利用されていた。

悪意あるドメインのスコアが高いレジストラTOP15(2013年上半期)

全てのレジストラにおいて25件以上の悪意あるドメイン登録が行われており、
且つgTLD下にある50,000個以上のドメイン名を管理している。

順位	レジストラ名	悪意あるドメイン数	管理下にあるドメイン数(2013年5月)	ドメイン10,000個あたりの悪意あるドメイン数
1	Shanghai Yovole Networks Inc. (中国)	1,235	332,064	37.2
2	Hang Zhou E-Business Services Co. Ltd. (中国)	177	104,741	16.9
3	Beijing Innovative Linkage Technology Ltd. Dba DNS.com.cn (中国)	607	405,491	15.0
4	Jiangsu Bangning Science & Technology Co. Ltd. (中国)	572	390,053	14.7
5	Web Commerce Communications dba Webnic.cc (マレーシア)	160	318,678	5.0
6	1API GmbH (ドイツ)	113	241,203	4.7
7	Xin Net Technology Corporation (中国)	382	1,459,147	2.6
8	Bizcn.com Inc. (中国)	125	505,802	2.5
9	DotTK	2,801	16,100,000	1.7
10	Domain.com LLC dba Dotster (アメリカ)	310	2,036,287	1.5

11	PDR Ltd. Dba Publicdomainregistry.com (インド)	478	3,147,935	1.5
12	Hichina Zhicheng Technology (中国)	208	1,669,183	1.2
13	OVH (フランス)	113	1,418,822	0.8
14	Register.com (アメリカ)	166	2,627,028	0.6
15	eNom (アメリカ)	612	11,751,759	0.5
順位	レジストラ名	悪意あるドメイン数	管理下にあるドメイン数 (2013年5月)	ドメイン10,000個あたりの悪意あるドメイン数

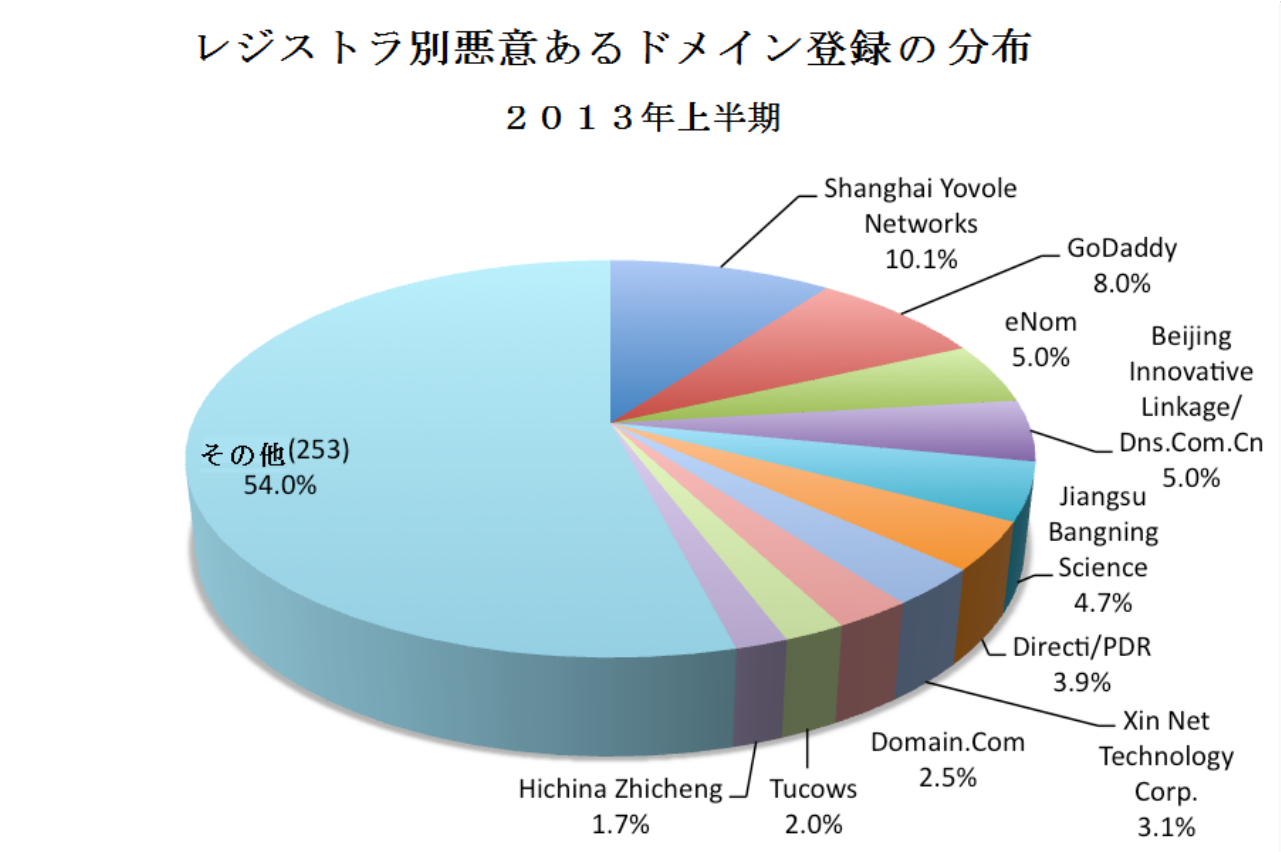
悪意あるドメイン登録のおよそ25パーセントは.TKレジストリで行われていた。これと同時に.TKレジストリはレジストラとしてドメイン登録を無料で行っている。レジストリにあるドメイン数が非常に多いため、.TKにおける悪意ある登録は相対的に小さくなり10,000ドメインあたり1.7であった。

これまでの傾向に引き続き、上位レジストラ12社の内8社は中国で設立されている。そのため、中国系フィッシング詐欺者はフィッシングを行う際にドメイン登録を行う傾向にあり、また頻繁に中国のレジストラを利用しているのである。中国のレジストラが登録したドメイン名は、AlibabaやTaobao.comそしてCCTVといった中国にある企業・組織を標的にした攻撃にだけでなくFacebookやPayPalなどの中国国外の企業・組織を標的にした攻撃にも使われていた。国内の標的に対して攻撃を行うために国外のレジストラでもドメイン登録を行っていたが、ほとんどのドメイン登録を中国にあるレジストラを通して行っていた。フィッシングのために登録された.CN下のドメイン名は165個(殆どは中国のレジストラにより登録されていた)で2012年下半期から著しく上昇した。

他を圧倒するレジストラが存在する。上記表のトップの座に着いているShanghai Yovole Networks Inc. (http://www.yovole.com/)だ。Shanghai Yovole Networks Inc.の10,000個当りのスコアは749から37と著しく改善しているものの、これは悪意あるドメインより遥かに多い無害なドメインを管理下においた結果であると思われる。スコアが10を超えた中国系レジストラは他に3社あった。中国系レジストラにとっては自社のサービスを通じてフィッシング詐欺者によるgTLD下のドメイン登録を防ぐことは未だ困難である。中国系レジストラを利用することは危険であるため、著者は中国系レジストラに対しAPWGが公開している「フィッシン

グ対策に関するレジストラ向けベストプラクティス勧告」の実行を推奨している。

通常より悪意ある登録が多いレジストラを見分ける方法として、管理下の10,000ドメインあたり１個以上悪意あるドメイン登録があるレジストラがおおよその指標となるだろう。我々は今後のレポートのためにデータを収集しつつも、この分野の研究を引き続き行っていき、よりよい調査方法を模索していくつもりだ。



サブドメインサービスを利用したフィッシング攻撃

サブドメインサービスを利用した攻撃は引き続き観測されてはいるものの、2013年上半期においてその数は再度減少した。中国系フィッシング詐欺者内では、「普通の」ドメイン名を登録することが好まれているため、サブドメインを登録するフィッシング詐欺者はほとんどいなかった。**しかしながら、サブドメインを利用したフィッシング攻撃は今なお全体の１０パーセントを占めている。**そのため我々は今後も、フィッシング詐欺者に利用される可能性のあるサブドメイン登録業者の観測を続けていく。

本報告書では「サブドメイン登録事業者」を「登録業者が所有するドメイン名の下に、顧客に対してサブド

メインの『ホスティングアカウント』を付与している事業者」と定義する。サブドメインサービスにより、登録業者は業者の所有するDNS空間において、様々な目的に合わせて顧客に対してサブドメイン名を効率的に登録することができる。更には登録したサブドメインの管理権限も無料で付与している。そのため、顧客は自身のウェブサーバーやメールサーバーを以下のようなホスト名にすることができる。
<顧客が指定した文字列>.<登録業者が所有するドメイン名>.TLD

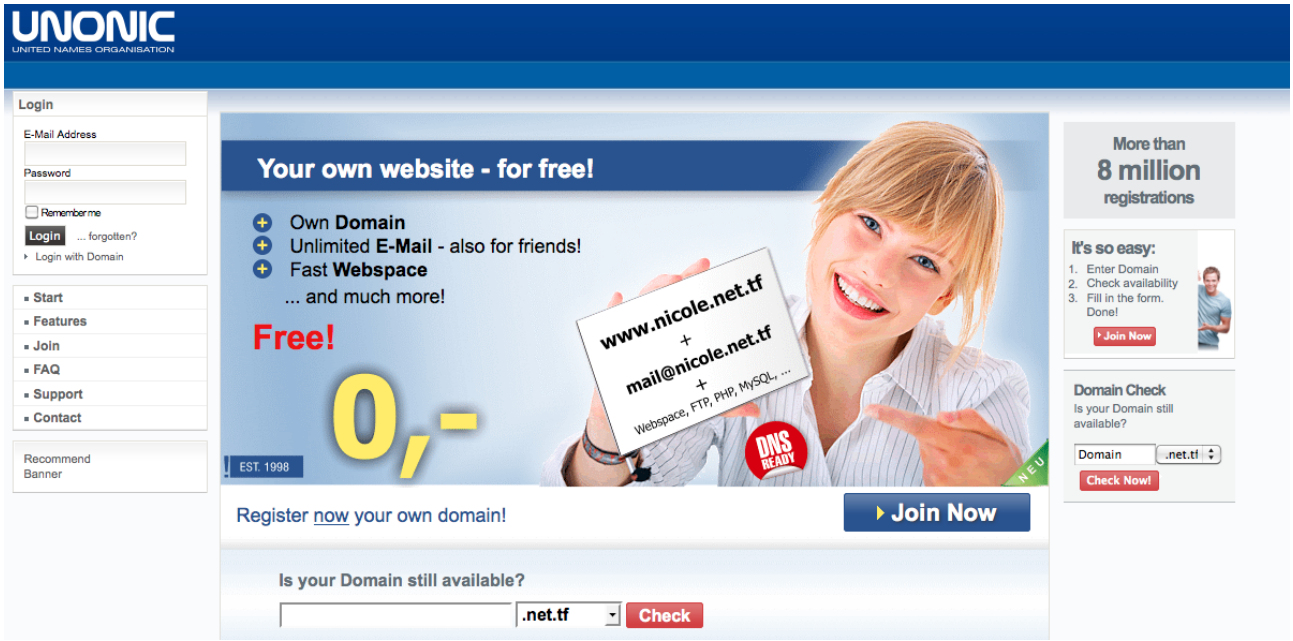
事業者の多くは無料且つ匿名でのサブドメインの登録を受け付けており、またサブドメイン登録事業者しか効率的にフィッシングの影響を低減することができない[9]ため、サブドメインサービスを利用することは未だ危険性を孕んでいる。事業者の多くは顧客からのフィッシング報告を受け付けているが、そのフィッシングに対する対応策は限られている。

2013年上半期において、7,134個のフィッシングサイトがサブドメイン登録事業者の持つ6,465個の異なるサブドメイン上にホストされていた。2012年下半期の8,294個からは14パーセント減少したものの、この数値は2013年上半期に発生した全フィッシング攻撃の10パーセントを未だ占めている。フィッシングに使われる技術全体に対し、サブドメインを利用した攻撃が増えているにもかかわらず、サブドメインの絶対数は減少を続けている。より多くのドメイン事業者が悪用を防止、検知、対応するシステムを導入していることが減少の理由の一つとして上げられるだろう。

多数の新規サブドメイン登録事業者が、フィッシング詐欺者に悪用されていることがわかった。**2013年上半期において270以上のサブドメイン登録事業者がフィッシング攻撃に利用されており、この数字は過去の報告書でも例がない数値である。**フィッシング詐欺者にとっては「新天地」となるドメインにおいておよそ1,270件の攻撃が報告された。もし、貴方がサブドメイン登録事業を新規に立ち上げたならば、彼らがそれを利用して攻撃を行うことは明々白々だろう。

2013年上半期において最も悪用の被害を受けたサブドメイン登録事業者はトイツ企業であるUNONICだった。UNONICには少なくとも865個の悪意あるサブドメインが登録されていた。過去の調査から、フィッシング詐欺者は脆弱だと判断したドメイン登録事業者のみを悪用しているため、UNONICが悪意あるサブドメインの温床として注視されることはなかった。UNONICはサブドメイン登録を無料で受け付けており、様々な登録可能なサブドメインを.tf(フランス領南方、南極地域のTLD)ドメイン下に多数保有しているが、UNONICのウェブサイトは堅牢な上、悪用報告窓口が設置されているにも関わらず、2013年上半期においてここまで悪用されているとは些か驚きだ。これは「表向きの」対策がフィッシング詐欺者を防ぐに至らないためであろう。

9 レジストラ若しくはレジストリの運営側は通常、フィッシングの影響を低減させることができない。というのも、影響を抑えるためにフィッシングサイトがあるサブドメインのメインドメイン即ち「親ドメイン」を停止させてしまうと、その親ドメイン下にホストされている全てのサブドメインも同時に無効化されてしまい、更には関係のないユーザーまでもが影響を受けてしまう可能性があるためだ。しかし、大規模なドメインの悪用がひとつのドメイン上で発生した際に、レジストラに多数のユーザーから報告が寄せられた場合には親ドメインを停止させることも選択肢の一つとして残っている。この状況は時折観測されている。



下表第2位のサブドメイン登録事業者である「3owl.com」は、かつて最も悪用されているとみなされていた。この業者は今日のインターネット上にある数多の「乱れ」を体現している。例えば、事業者の本拠地や、事業従事者が悪用防止措置を取っているのかが非常に不明瞭である。また、3owl.comのWHOISデータはGoDaddyドメイン上では「プライバシー保護」がされており、なおかつ3owl.comの本部サイト上に直接の連絡先が記されていない。それ以外にも、本部サイトの「プライバシーポリシー」と「概要」のハイパーリンクは広告にリンクされているため、顧客に対して事業説明が全くなされていない。　悪用を報告する窓口はあるものの、利用者が本当に悪用報告に注意を払っているかは不明である。

また、Googleが運営するBlogSpot.comというブログサービスも興味深い。このブログサイトにおいて特筆すべき悪用されたサブドメインはないが、このサービス上で見つかったフィッシングサイトが2013年上半期で延べ300個にまで昇った。Googleは、悪用報告に対し即座に対応することに関して長期にわたり問題を抱えている。

フィッシングに使われた回数の多いサブドメイン登録事業者　(2013年上半期)

順位	攻撃に利用された回数	ドメイン名	業者名
1	833	net.tf	UNONIC.COM
2	347	3owl.com	3owl.com
3	290	usa.cc	freeavailabledomains.com
4	240	nazuka.net	nazuka.net

5	226	altervista.org	altervista.org
6	193	my3gb.com	my3gb.com
7	155	kmdns.net	kmdns.net
8	137	3eeweb.com	3eeweb.com
9	92	p.ht	Hostinger
10	89	cixx6.com	cixx6.com
11	81	wink.ws	wink.ws
12	66	instantfreesite.com	instantfreesite.com
13	62	5gbfree.com	5gbfree.com
14	62	chickenkiller.com	chickenkiller.com
15	55	fav.cc	fav.cc
16	55	ias3.com	ias3.com
17	50	co.vu	co.vu
18	48	oicp.net	Oray
19	46	hol.es	Hostinger
20	45	vicp.cc	Oray

800を超えるサブドメイン登録事業者が、3,800個以上の固有なドメイン名上でサービスを提供していることがわかっている。各登録事業者はサブドメインのレジストラでありながら同時にレジストリでもある。サブドメイン登録事業には数多くのビジネスモデルがあるが、未だ野放しのまま規制がなされていない。TLDのレジストリやレジストラが悪用防止策を導入するにつれ、フィッシング詐欺者がこうしたサブドメイン空間に移行することは驚くべきことではない。

国際化ドメイン名(IDN)を利用したフィッシング攻撃

過去の調査に続き、今回の調査データでも国際化ドメイン名（IDN）が持つ独自の特徴を利用した有意なフィッシング攻撃はほとんど行われていないことがわかった。

国際化ドメイン名（以下IDN）とは、ドメイン名にASCII以外の文字コードを含めることができる仕組みのことだ。具体的に言えば、á やüといったダイアクリティカルマークが付与された文字やアラビア文字、漢字、キリル文字そしてデーヴァナーガリー文字（ヒンディ語で使われる）などの非ラテン文字をドメイン名として使うことができる。7年以上前から、多くのレジストリの第二、第三レベルドメインにおいてIDNを利用することができ、IDNの大多数はアジア地域で登録されている。IDN TLD(国際化TLD名)ではTLDを含めたドメ

イン名全体にラテン文字以外を使用することができる。ユーザーは、ユーザーが普段用いる言語以外の文字についてはほとんど(若しくは全く)認識できないため、フィッシング詐欺者はこれを用いてドメイン名をブランド名に偽装しユーザーを騙すIDN同形異義語攻撃を行っている。しかし、2007年1月から2012年12月に渡り、IDNを利用したフィッシング攻撃はわずか5件のみだった。
2013年春においては以下の3件の同形異義語攻撃を検知した。

xn--paypl-uqa.com ・ paypàl.com

xn--tunes-4sa.eu ・ îtunes.eu

xn--tunes-bta.fr ・ ïtunes.fr

長年にわたりIDNは広く使われてきているにもかかわらず、何故フィッシング詐欺者はIDNを用いた同形異義語攻撃を滅多に行わないのだろうか。
1. 同形異義語攻撃に頼る「必要性」がない。本報告書の中で述べられているように、ドメイン名自体はフィッシング詐欺者に取ってはさほど重要ではないため。
2.一部のウェブブラウザではドメイン名をアドレスバーにそのまま表示するのではなく、Punycodeを用いて表示するようにデフォルトでなっているため(例："xn--hotmal-t9a.net")。それ故、それらのウェブブラウザを使用するユーザーは偽装されたドメイン名を見ることがない。

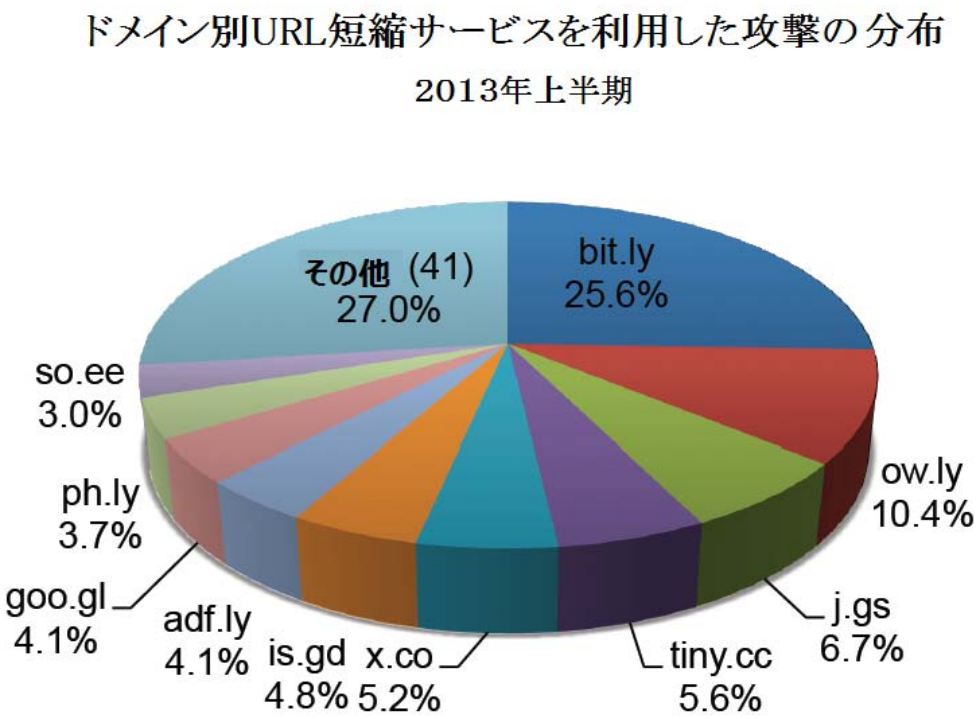
2013年後半以降、IDN対応の新しいレジストリが複数追加されることになっているため、我々はこの興味深い傾向を引き続きモニタリングしていく。

URL 短縮サービスを利用したフィッシング攻撃

フィッシングサイトのURLであるとわかり難くさせるために、URL短縮サービスが引き続き用いられている。しかし、このサービスを用いた攻撃は2013年上半期においてわずか270件で2012年下半期の785件から大幅に落ち込んだ。URL短縮サービスを利用することで、本来は長大なURLを文字数が限られている投稿フォームなどに挿入することができる。この短縮されたURLを閲覧者がクリックすると本来の文字数の多い「隠れた」URLに自動的にリダイレクトされる。

この大幅な減少は、主要なURL短縮サービスのほとんどが悪意ある転送先のスクリーニングを強化し、より容易にそして効果的に悪用を報告できるようにしたことの証明となっているのだろう。ベストプラクティスとして、URL短縮サービスの多くは迅速に転送先URLを特定できるツールや自動的に悪用を通報する機能を提供している。我々はURL短縮サービスの提供者に対し同様の対策を実施し、改善し続けることを奨励している。

SURBL (http://www.surbl.org)はURL短縮サービスの悪用に関する情報を無料で提供している。URL短縮サービスを提供する全ての者は、各自のサービスが悪用されるのを防ぐ為にこのサイトへの登録を検討してほしい。非常に多くの短縮URLがマルウェアを利用したエクスプロイトキットが含まれたサイトにリダイレクトされている。本報告書の範囲外ではあるが、この問題が現時点で本当に「解決できる」かについては些か疑問が残る。



過去の報告書では、フィッシングに使われた悪意ある短縮URLの65パーセント超はたったひとつのURL短縮サービスで見つかった。tinyURL.comだ。tinyURL.comは非常に人気のあるURL短縮サイトであるが、サポートは限らており、また、悪用を通報する窓口がウェブサイト上に存在していなかった。 サポートを拡充か、或いは窓口を設置したのか、tinyURL.comは本報告書には一切登場していない。これは恒久対策であり、うまくいけば産業全体に有益なものとなるだろう。2013年上半期ではURL短縮サービスの悪用は全体として非常に少なかった。しかし、Bit.lyを利用した短縮URLのおよそ25%が悪意あるドメイン名にリダイレクトされていた。

スピア型フィッシング攻撃について

本報告書は一般公衆を標的にしたフィッシング攻撃を対象にしているが、特定の個人・組織を狙った攻撃であるスピア型フィッシング攻撃は含まれていない。これには理由として、第一に標的をおびき寄せるメールの数が極少数であること、第二に企業の内部システムを標的にすること、第三にスピア型フィッシングの攻撃未遂は一般的には通報されないこと。そして第四にどれほど多くのスピア型フィッシング攻撃が行われているか不明なことがあげられる。スピア型フィッシング攻撃は以下の者にとっては重要な攻撃手段である。

- 金融犯罪を企てる犯罪者。例えば、フィッシング詐欺者が標的となった大学の職員に対しパスワードを漏洩させ、給与明細が格納されている場所への転送先を書き換える等。
- 政府や企業の諜報部に所属しているスパイ。2013年2月、コンピューターセキュリティ会社であるMandiantは、中国軍部のハッカーによるスピア型フィッシング攻撃を検知した。
- 主義・主張を公衆に知らせんとするハクティビスト(政治的ハッカー)。2013年8月27日、親アサド派であるシリア電子軍(SEA)のメンバーが、雑でありながら効果的なスピア型フィッシング攻撃を行い、とあるリセラのログイン証明書を入手した。SEAはそのリセラのシステムに侵入し、New York Times紙のウェブサイトではなくSEAが作成したウェブサイトに転送されるようにDNS記録を書き換えた。

付録:TLD 毎のフィッシング統計＆稼働時間

TLD 名	TLD 地域	固有なフィッシング攻撃件数（2013 年上半期）	フィッシングに利用された固有なドメイン名数（2013 年上半期）	レジストリ内ドメイン数（2013 年 4 月）	スコア:10,000 ドメインあたりのフィッシングドメイン（2013 年上半期）	スコア:10,000 ドメインあたりのフィッシング攻撃（2013 年上半期）	攻撃の平均稼働時間 hh:mm（2013 年上半期）	攻撃の稼働時間中央値（2013 年上半期）	2013 年上半期に登録された悪意ある総ドメイン数	スコア：レジストリ下 10,000 ドメインあたりの悪意あるドメイン登録
ac	アセンション島	2	2	16,100	1.2	1.2	2:49	2:49		
ad	アンドラ			1,500						
ae	アラブ首長国連邦	42	23	102,000	2.3	4.1	245:15	56:38	2	0.2
aero	スポンサー付 TLD	2	2	8,586	2.3	2.3	8:10	8:10		
af	アフガニスタン									
ag	アンティグア・バーブーダ	1	1	19,598	0.5	0.5	185:27	185:27		
ai	アンギラ	2	2	3,900	5.1	5.1	16:11	16:11		
al	アルバニア	1	1	7,500	1.3	1.3	0:18	0:18		
am	アルメニア	57	9	22,327	4	25.5	17:30	2:15	1	0.4
an	オランダ領アンティル			800						
ao	アンゴラ			300						
ar	アルゼンチン	493	425	2,900,000	1.5	1.7	38:33	14:52	6	0
arpa	逆引き(アメリカ国防総省国防高等研究計画局)									
as	アメリカ領サモア									
asia	スポンサー付 TLD	361	240	474,322	5.1	7.6	31:52	7:58	171	3.6
at	オーストリア	74	60	1,201,000	0.5	0.6	59:32	16:47		
au	オーストラリア	865	767	2,639,461	2.9	3.3	49:59	12:18	17	0.1
aw	アルバ	3	1	625	16	48	145:23	139:37		
ax	オーランド諸島									
az	アゼルバイジャン	5	4	17,950	2.2	2.8	40:19	5:32		
ba	ボスニア・ヘルツェゴビナ	20	12	14,589	8.2	13.7	33:11	22:54	1	0.7
bd	バングラデシュ	23	15	5,000	30	46	35:27	22:21		
be	ベルギー	200	157	1,368,637	1.1	1.5	54:50	14:50	11	0.1
bf	ブルキナファソ	1	1				12:50	12:50		
bg	ブルガリア	9	7	25,000	2.8	3.6	13:30	4:21		

TLD 名	TLD 地域	固有なフィッシング攻撃件数（2013 年上半期）	フィッシングに利用された固有なドメイン名数（2013 年上半期）	レジストリ内のドメイン数（2013 年 4 月）	スコア:10,000 ドメインあたりのフィッシングドメイン（2013 年上半期）	スコア:10,000 ドメインあたりのフィッシング攻撃（2013 年上半期）	攻撃の平均稼働時間 hh:mm（2013 年上半期）	攻撃の稼働時間中央値（2013 年上半期）	2013 年上半期に登録された悪意ある総ドメイン数	スコア：レジストリ下 10,000 ドメインあたりの悪意あるドメイン登録
bh	バーレーン			4,450						
biz	分野別 TLD	436	324	2,400,109	1.3	1.8	37:15	18:12	52	0.2
bm	バミューダ			8,100						
bn	ブルネイ	1	1	1,150	8.7	8.7	538:29	538:29		
bo	ボリビア	8	5	8,350	6	9.6	24:15	9:16		
br	ブラジル	3,668	2,669	3,265,768	8.2	11.2	45:21	15:31	114	0.3
bs	バハマ			2,320						
bt	ブータン	11	9	1,090	82.6	100.9	29:52	16:08		
bw	ボツワナ									
by	ベラルーシ	50	37				67:27	17:42	3	
bz	ベリーズ	5	5	44,703	1.1	1.1	18:16	18:47	1	0.2
ca	カナダ	500	407	2,042,762	2	2.4	53:38	15:42	10	0
cat	スポンサー付 TLD	13	11	65,543	1.7	2	245:31	30:03	1	0.2
cc	ココス(キーリング)諸島(概算値)	573	70	800,000	0.9	7.2	45:51	6:02	16	0.2
cd	コンゴ民主共和国(概算値)	3	3	5,200	5.8	5.8	103:18	66:57		
cf	中央アフリカ									
cg	コンゴ共和国									
ch	スイス	114	85	1,774,262	0.5	0.6	72:45	17:16	2	0
ci	コートジボワール			2,500						
cl	チリ	494	357	418,558	8.5	11.8	51:23	16:29	8	0.2
cm	カメルーン(概算値)		9	6	12,500	4.8	21:51	0:00	0:00	
cn	中国	491	387	7,544,052	0.5	0.7	29:53	10:56	165	0.2
co	コロンビア	311	263	1,386,328	1.9	2.2	24:53	12:56	26	
com	分野別 TLD	34,867	27,684	111,163,489	2.5	3.1	43:26	12:27	6,479	0.6
coop	スポンサー付き TLD	2	2	9,983	2	2	30:18	30:18		
cr	コスタリカ	8	7	14,800	4.7	5.4	8:02	5:35		
cu	キューバ			2,370						
cv	カーボベルデ			900						

TLD 名	TLD 地域	固有なフィッシング攻撃件数（2013 年上半期）	フィッシングに利用された固有なドメイン名数（2013 年上半期）	レジストリ内のドメイン数（2013 年 4 月）	スコア:10,000 ドメインあたりのフィッシングドメイン（2013 年上半期）	スコア:10,000 ドメインあたりのフィッシング攻撃（2013 年上半期）	攻撃の平均稼働時間 hh:mm（2013 年上半期）	攻撃の稼働時間中央値（2013 年上半期）	2013 年上半期に登録された悪意ある総ドメイン数	スコア：レジストリ下 10,000 ドメインあたりの悪意あるドメイン登録
cx	クリスマス島	15	6	5,250	11.4	28.6	5:42	2:40		
cy	キプロス	1	1	12,500	0.8	0.8				
cz	チェコ	111	73	1,048,161	0.7	1.1	67:08	12:33		
de	ドイツ	914	771	15,397,225	0.5	0.6	56:03	15:57	121	0.1
dj	ジブチ									
dk	デンマーク	172	113	1,242,409	0.9	1.4	63:01	19:08	2	0
dm	ドミニカ国			14,500						
do	ドミニカ共和国	21	13				22:19	19:05	1	
dz	アルジェリア	1	1	4,665	2.1	2.1	34:06	34:06		
ec	エクアドル	64	48	30,500	15.7	21	28:31	13:31	1	0.3
edu	米国高等教育機関	13	7	7,590	9.2	17.1	31:49	13:35		
ee	エストニア	33	21	69,750	3	4.7	34:00	22:04		
eg	エジプト	2	2	6,000	3.3	3.3				
er	エリトリア			120						
es	スペイン	305	202	1,648,082	1.2	1.9	44:56	7:53	6	0
et	エチオピア	1	1	1,200	8.3	8.3				
eu	欧州連合（EU）	325	275	3,723,077	0.7	0.9	35:49	12:08	53	0.1
fi	フィンランド	35	22	316,422	0.7	1.1	203:58	78:45		
fj	フィジー	5	2	4,000	5	12.5				
fk	フォークランド諸島			105						
fm	ミクロネシア	10	9				26:05	7:55		
fo	フェロー諸島									
fr	フランス	451	325	2,601,215	1.2	1.7	61:35	18:13	31	0.1
gd	グレナダ	17	3	4,400	6.8	38.6	19:45	8:38		
ge	グルジア	61	41	20,300	20.2	30	101:25	89:04	6	3
gg	ガーンジー	30	4							
gh	ガーナ	5	2				32:38	20:38		
gi	ジブラルタル			2,033						

TLD 名	TLD 地域	固有なフィッシング攻撃件数(2013 年上半期)	フィッシングに利用された固有なドメイン名数(2013 年上半期)	レジストリ内のドメイン数(2013 年 4 月)	スコア:10,000 ドメインあたりのフィッシングドメイン(2013 年上半期)	スコア:10,000 ドメインあたりのフィッシング攻撃(2013 年上半期)	攻撃の平均稼働時間 hh:mm(2013 年上半期)	攻撃の稼働時間中央値(2013 年上半期)	2013 年上半期に登録された悪意ある総ドメイン数	スコア : レジストリ下 10,000 ドメインあたりの悪意あるドメイン登録
gl	グリーンランド	13	2	5,500	3.6	23.6	32:01	1:07		
gm	ガンビア									
gov	米政府	1	1	5,000	2	2	21:59	21:59		
gp	グアドループ	10	8	1,475	54.2	67.8	10:08	7:29		
gr	ギリシャ(概算値)	203	162	377,000	4.3	5.4	58:48	13:04	6	0.2
gs	サウスジョージア・サウスサンドウィッチ諸島	24	5	8,160	6.1	29.4	25:06	9:42	1	1.2
gt	グアテマラ	14	11	11,900	9.2	11.8	58:24	9:04	1	0.8
gy	ギニア	7	1	2,300	4.3	30.4				
hk	香港	34	17	245,151	0.7	1.4	125:01	26:47	4	0.2
hm	ハード島及びマクドナルド島									
hn	ホンジュラス	3	1	6,300	1.6	4.8	40:54	26:55	1	1.6
hr	クロアチア	30	29	79,094	3.7	3.8	27:31	12:26		
ht	ハイチ	94	3	2,200	13.6	427.3	23:45	0:00		
hu	ハンガリー	190	143	631,189	2.3	3	72:56	18:29	4	0.1
id	インドネシア	98	72	109,000	6.6	9	30:10	9:16	1	0.1
ie	アイルランド	88	64	183,550	3.5	4.8	84:19	19:10	1	0.1
il	イスラエル	55	44	237,155	1.9	2.3	55:16	14:26	1	0
im	マン島	13	9	1			28:36	20:57	1	
in	インド	686	564	1,283,554	4.4	5.3	39:11:	12:30	75	0.6
info	分野別 TLD	1,561	1,308	6,774,502	1.9	2.3	30:00:	11:17	655	1
int	スポンサー付 TLD									
io	イギリス領インド洋地域	3	2							
IP	IP アドレス(ドメイン名でない)	1,972								
iq	イラク			450						
ir	イラン	188	150	393,689	3.8	4.8	21:22	9:36	11	0.3
is	アイスランド	13	12	42,500	2.8	3.1	42:25	13:10		
it	イタリア	383	307	2,500,000	1.2	1.5	73:39	20:53	8	0
je	ジャージー島									

TLD 名	TLD 地域	固有なフィッシング攻撃件数（2013 年上半期）	フィッシングに利用された固有なドメイン名数（2013 年上半期）	レジストリ内のドメイン数（2013 年 4 月）	スコア:10,000 ドメインあたりのフィッシングドメイン（2013 年上半期）	スコア:10,000 ドメインあたりのフィッシング攻撃（2013 年上半期）	攻撃の平均稼働時間 hh:mm（2013 年上半期）	攻撃の稼働時間中央値（2013 年上半期）	2013 年上半期に登録された悪意ある総ドメイン数	スコア：レジストリ下 10,000 ドメインあたりの悪意あるドメイン登録
jm	ジャマイカ	2	1	6,400	1.6	3.1				
jo	ヨルダン	2	1	4,341	2.3	4.6	34:14	34:14		
jobs	スポンサー付き TLD	0	0	44,057						
jp	日本	111	89	1,334,594	0.7	0.8	55:07	15:10	3	0
ke	ケニア	60	48	25,345	18.9	23.7	42:47	20:45	6	2.4
kg	キルギス	1	1	5,300	1.9	1.9				
kh	カンボジア	7	7	1,600	43.8	43.8	10:26	11:37		
ki	キリバス									
kn	セントクリストファー・ネイビス	4	4	2			51:26	15:02		
kr	韓国	260	147	1,173,900	1.3	2.2	59:13	16:47	4	0
kw	クウェート	1	1	3,350	3	3	10:43	10:43		
ky	ケイマン諸島	1	1				3:39	3:39		
kz	カザフスタン	67	55	88,608	6.2	7.6	20:59	15:02	1	0.1
la	ラオス（ドメイン数は概算値）		8	6	9,000	6.7	8.9	52:18	7:44	
lb	レバノン	2	1	3,500	2.9	5.7	11:20	11:20		
lc	セントルシア	11	9	3,784	23.8	29.1	30:26	1:09		
li	リヒテンシュタイン	2	1	69,500	0.1	0.3	26:45	26:45		
lk	スリランカ	11	10	8,500	11.8	12.9	199:56	30:48		
ls	レソト									
lt	リトアニア	32	31	156,500	2	2	37:25	19:20	3	0.2
lu	ルクセンブルグ	10	8	74,500	1.1	1.3	83:56	59:44		
lv	ラトビア	45	33	105,500	3.1	4.3	27:05	11:37	2	0.2
ly	リビア	126	11	13,574	8.1	92.8	30:03	9:45	2	1.5
ma	モロッコ	44	33	43,299	7.6	10.2	118:38	15:37	3	0.7
mc	モナコ	1	1	2,370	4.2	4.2	65:13	65:13		
md	モルドヴァ	14	12	22,736	5.3	6.2	70:26	20:48		
me	モンテネグロ	246	90	678,096	1.3	3.6	32:14	7:43	11	0.2
mg	マダガスカル	1	1							

TLD 名	TLD 地域	固有なフィッシング攻撃件数（2013 年上半期）	フィッシングに利用された固有なドメイン名数（2013 年上半期）	レジストリ内のドメイン数（2013 年 4 月）	スコア:10,000 ドメインあたりのフィッシングドメイン（2013 年上半期）	スコア:10,000 ドメインあたりのフィッシング攻撃（2013 年上半期）	攻撃の平均稼働時間 hh:mm（2013 年上半期）	攻撃の稼働時間中央値（2013 年上半期）	2013 年上半期に登録された悪意ある総ドメイン数	スコア：レジストリ下 10,000 ドメインあたりの悪意あるドメイン登録
mk	マケドニア	22	18	2,266	79.4	97.1	40:49	7:54		
ml	マリ	1	1				37:53	37:53		
mn	モンゴル	17	13	14,551	8.9	11.7	27:00	9:40		
mo	マカオ	8	5	305	163.9	262.3	910:50	1313:49		
mobi	スポンサー付き TLD	60	44	1,078,020	0.4	0.6	25:22	10:02	5	0
mp	北マリアナ諸島									
mr	モーリタニア	1	1				7:55	7:55		
ms	モントセラト	113	11	9,800	11.2	115.3	27:35	17:32		
mt	マルタ（概算値）	1	1	6,250	1.6	1.6	149:59	149:59		
mu	モーリシャス	74	4	7,500	5.3	98.7	19:12	2:03		
museum	スポンサー付き TLD			435						
mv	モルディブ	1	1				166:27	166:27		
mx	メキシコ	321	254	669,414	3.8	4.8	71:13	15:55	26	0.4
my	マレーシア	153	112	202,869	5.5	7.5	38:49	12:57	5	0.2
mz	モザンビーク	0	0	4,000						
na	ナミビア	1	1							
name	分野別TLD	52	40	214,831	1.9	2.4	22:41	6:36	9	0.4
nc	ニューカレドニア	2	1				43:21	43:21		
ne	ニジェール									
net	分野別 TLD	4,640	3,228	15,449,095	2.1	3	40:39	11:04	560	0.4
nf	ノーフォーク島	12	3	1,600	18.8	75	40:25	3:06		
ng	ナイジェリア	12	12	12,500	9.6	9.6	35:00	20:33	2	1.6
ni	ニカラグア	0	0	6,600						
nl	オランダ	443	375	5,243,494	0.7	0.8	35:19	10:46	31	0.1
no	ノルウェイ	80	56	581,386	1	1.4	71:29	20:33		
np	ネパール	97	64	32,500	19.7	29.8	95:37	21:45		
nr	ナウル	1	1	450	22.2	22.2				
nu	ニウエ（ドメイン数は概算値）	59	24	100,000	2.4	5.9	56:37	0:34	2	0.2
nz	ニュージーランド	102	86	530,479	1.6	1.9	35:23	10:40	1	0
om	オマーン	2	2				22:23	22:23	1	

TLD 名	TLD 地域	固有なフィッシング攻撃件数（2013 年上半期）	フィッシングに利用された固有なドメイン名数（2013 年上半期）	レジストリ内のドメイン数（2013 年 4 月）	スコア:10,000 ドメインあたりのフィッシングドメイン（2013 年上半期）	スコア:10,000 ドメインあたりのフィッシング攻撃（2013 年上半期）	攻撃の平均稼働時間 hh:mm（2013 年上半期）	攻撃の稼働時間中央値（2013 年上半期）	2013 年上半期に登録された悪意ある総ドメイン数	スコア：レジストリ下 10,000 ドメインあたりの悪意あるドメイン登録
org	分野別 TLD	2,743	2,032	10,258,953	2	2.7	31:09	12:03	226	0.2
pa	パナマ	2	2	7,200	2.8	2.8	6:03	6:03		
pe	ペルー	143	107	69,505	15.4	20.6	29:41	19:22	2	0.3
pf	フランス領ポリネシア	2	1							
ph	フィリピン （運営側が管理下のドメイン数提供を拒否）	28	20				42:33	17:37		
pk	パキスタン （運営側が管理下のドメイン数提供を拒否）	238	176				35:38	13:47	2	1.1
pl	ポーランド	720	507	2,440,637	2.1	3	50:10	14:58	18	0.1
pn	ピトケアン島	65	6				3:26	4:11		
post	スポンサー付き TLD			8						
pro	スポンサー付き TLD	33	24	156,639	1.5	2.1	24:37	8:32	3	0.2
ps	パレスチナ領	5	5	7,150	7	7	30:48	21:46		
pt	ポルトガル	114	86	236,950	3.6	4.8	66:53	19:01	6	0.3
pw	パラオ	115	109	55,000	19.8	20.9	31:13	12:41	94	17.1
py	パラグアイ	19	18	14,520	12.4	13.1	17:28	11:22	2	1.4
qa	カタール	1	1	15,008	0.7	0.7				
re	レユニオン島	3	3	20,826	1.4	1.4	11:00	13:25	2	1
ro	ルーマニア	341	259	641,700	4	5.3	60:02	11:18	4	0.1
rs	セルビア	59	45	77,133	5.8	7.6	47:41	16:52	3	0.4
ru	ロシア	1,011	772	4,510,050	1.7	2.2	52:53	13:22	78	0.2
rw	ルワンダ									
sa	サウジアラビア	40	33	30,400	10.9	13.2	30:25	20:00		
sc	セーシェル	1	1	4,915	2	2	16:11	16:11	1	2
sd	スーダン	10	9				5:06	7:01		
se	スウェーデン	167	127	1,281,322	1	1.3	73:38	16:37	1	0
sg	シンガポール	83	52	148,001	3.5	5.6	114:58	18:52	3	0.2
sh	セントヘレナ	3	1	3,000	3.3	10	134:39	136:37:00	1	3.3
si	スロベニア	219	196	108,100	18.1	20.3	47:20	6:27		
sk	スロバキア	67	41	292,572	1.4	2.3	86:23	14:35		

TLD 名	TLD 地域	固有なフィッシング攻撃件数（2013 年上半期）	フィッシングに利用された固有なドメイン名数（2013 年上半期）	レジストリ内のドメイン数（2013 年 4 月）	スコア:10,000 ドメインあたりのフィッシングドメイン（2013 年上半期）	スコア:10,000 ドメインあたりのフィッシング攻撃（2013 年上半期）	攻撃の平均稼働時間 hh:mm（2013 年上半期）	攻撃の稼働時間中央値（2013 年上半期）	2013 年上半期に登録された悪意ある総ドメイン数	スコア：レジストリ下 10,000 ドメインあたりの悪意あるドメイン登録
sl	シエラレオネ									
sm	サンマリノ	0	0	1,905						
sn	セネガル	1	1	3,500	2.9	2.9	45:29	45:29		
so	ソマリア	9	5				190:01	140:25	4	
sr	スリナム	1	1							
st	サントメ・プリンシペ	2	2				3:39	3:39		
su	ソビエト連邦	73	31	120,100	2.6	6.1	33:47	9:09	2	0.2
sv	エルサルバドル	10	9	6,500	13.8	15.4	62:21	18:45		
sy	シリア									
sz	スワジランド									
tc	タークス・カイコス諸島	8	3				5:09	5:09		
tel	分野別 TLD	0	0	211,979						
tf	フランス領南方南極地域	949	14	1,550	90.3	6122.6	38:31	22:38	1	6.5
tg	トーゴ									
th	タイ	166	125	65,350	19.1	25.4	27:43	13:21	2	0.3
tj	タジキスタン	2	2	6,200	3.2	3.2	29:34	29:34		
tk	トケラウ	3,077	2,802	16,100,000	1.7	1.9	17:38	7:19	2,801	1.7
tl	東ティモール	3	3				2:54	2:43		
tm	トルクメニスタン	43	4	3,780	10.6	113.8	31:33	21:16	1	2.6
tn	チュニジア	15	12	16,950	7.1	8.8	115:56	42:16		
to	トンガ	24	13	15,500	8.4	15.5	60:49	36:43		
tp	ポルトガル領ティモール									
tr	トルコ	193	153	333,508	4.6	5.8	43:58	17:39	3	0.1
travel	スポンサー付き TLD	0	0	20,671						
tt	トリニダード・トバゴ			2,525						
tv	ツバル（概算値）	69	55	175,000	3.1	3.9	27:24	13:45	1	0.1
tw	台湾	85	64	630,550	1	1.3	77:46	25:05	4	0.1
tz	タンザニア	10	8	6,220	12.9	16.1	66:32	23:15		
ua	ウクライナ	289	246	700,013	3.5	4.1	30:37	12:06	10	0.1
ug	ウガンダ	23	11	3,200	34.4	71.9	65:22	31:16	1	3.1

TLD 名	TLD 地域	固有なフィッシング攻撃件数（2013 年上半期）	フィッシングに利用された固有なドメイン名数（2013 年上半期）	レジストリ内のドメイン数（2013 年 4 月）	スコア:10,000 ドメインあたりのフィッシングドメイン（2013 年上半期）	スコア:10,000 ドメインあたりのフィッシング攻撃（2013 年上半期）	攻撃の平均稼働時間 hh:mm:ss（2013 年上半期）	攻撃の稼働時間中央値（2013 年上半期）	2013 年上半期に登録された悪意ある総ドメイン数	スコア：レジストリ下 10,000 ドメインあたりの悪意あるドメイン登録
uk	イギリス	1,018	870	10,420,705	0.8	1	45:13	13:50	61	0.1
us	アメリカ	335	260	1,795,000	1.4	1.9	37:33	8:59	67	0.4
uy	ウルグアイ	16	16	74,605	2.1	2.1	31:21	16:37	1	0.1
uz	ウズベキスタン	5	4	16,387	2.4	3.1	17:49	0:58		
vc	セントビンセントおよびグレナディーン諸島	9	5	8,692	5.8	10.4	25:01	9:13		
ve	ベネズエラ	102	67	215,000	3.1	4.7	54:26	13:00	4	0.2
vg	イギリス領ヴァージン諸島	5	2	8,600	2.3	5.8	0:17	0:05		
vi	アメリカ領ヴァージン諸島			17,500						
vn	ベトナム	117	85	386,803	2.2	3	45:04	9:59		
vu	バヌアツ	88	5				39:42	12:51		
wf	ウォリス・フツナ	1	1				24:10	24:10		
ws	サモア(概算値)	131	39	450,000	0.9	2.9	23:35	4:51	4	0.1
xn--3e0b707	.한국(韓国の IDN)	0	0	91,300						
xn--90a3ac	.СРБ(セルビアの IDN)	0	0	5,175						
xn--fzc2c9e2c	(スリランカの IDN)	0	0	150						
xn--mgberp4a5d4a	サウジアラビアの IDN	0	0	1,850						
xn--o3cw4h	.ไทย	0	0	1,000						
xn--p1ai	.рф	4	3	788,675	0	0.1	0.1	7:52		
xn--xkc2al3hye2a	(スリランカの IDN)			86						
xxx	スポンサー付き TLD	3	3	108,337	0.3	0.3	99:21	99:21		
ye	イエメン			900						
yt	フランス									
za	南アフリカ	287	243	859,000	2.8	3.3	37:18	11:37	8	0.1
zm	ザンビア	2	2				7:17	7:17		
zw	ジンバブエ	7	5	1,050	47.6	66.7	9:51	5:04		
合計		**72,758**	**53,685**	**260,987,759**					**12,175**	

謝辞・著者紹介

本報告書作成にあたり、APWGメンバーのPeter Cassidy氏、 Foy Shiver氏 そしてInternet Identity社のAaron Routt氏には多大なるご協力をいただいたことを、ここに深く御礼申し上げたい。また、CNNICのLiming Wang氏、Wang Wei氏、Hu Anlei氏には、本報告書内におけるAPACのフィッシングデータに関して、DomainToolsにはWHOISデータを用いた悪意あるドメイン登録の傾向調査に関して多大なるご協力をいただいたことをここに、謝意を表したい。そして最後に、フィッシング対策・研究において取り組んでいるセキュリティ業界、ドメイン名業界、そして法執行機関の面々に対し、感謝申し上げたい。

Greg Aaron: インターネット企業やTLDレジストリ向けにコンサルティング及びセキュリティサービスを行うIllumintel社社長。インターネット犯罪におけるドメイン名利用に関する専門家で、レジストラやレジストリ、法執行機関、そして研究者と協力しフィッシング、マルウェア、スパム、そして児童ポルノの諸問題に取り組む。APWG内にあるインターネットポリシー委員会の共同委員長に就任中。ICANNを構成する一組織であるセキュリティと安定性に関する諮問委員会(SSAC)のメンバーで、過去には同じくICANNの構成組織である悪意あるドメイン登録に関する悪用対策実務者グループの委員長を務めた。以前はAfiliasの大口取引先管理及びドメインセキュリティ部取締役を務めていた。2010年、Online Trust Award(OTA)において、Afiliasのドメイン悪用対策プログラムに関してOTA優秀賞を受賞。政府やccTLDレジストリ、そしてICANNに対し、レジストリの方針・運営に関して助言を行い、.MOBI、.INそして.MEのTLD立ち上げを監督。またサンライズ期間(優先登録期間)やIDNの導入も手がけた。ペンシルベニア大学首席卒業生。

Rod Ramussen: Internet Identity社(www.internetidentity.com)社長兼最高技術責任者(CTO)であり、2001年共同設立当初から技術指導部として務める。犯罪者によるDNSの悪用問題の第一人者。APWG内にあるインターネットポリシー委員会の共同委員長に就任中で、同グループ内技術リエゾンとして仕え、同組織を代表し各国際行事に参加、講演を開いている。この役割の中で、ドメイン名に関する国際的取締団体であるICANNと密接に関与、セキュリティと安定性に関する諮問委員会(SSAC)及びgTLDディレクトリサービスに関するICANN専門家実務者グループのメンバーでもある。オンライントラストアライアンス運営委員会委員を務めており、米連邦通信委員会通信セキュリティ・信頼性・相互運用性評議会(FCC・CSRIC)メンバーに任命されたこともある。財界と法執行機関の協力により設立されたDigital Phishnet成員でもあり、MAAWG(Messaging Anti-Abuse Working Group)に積極的に参加しており、そしてFIRST(Forum of Incident Response and Security Teams)におけるInternet Identity社代表である。主要なDNS運営団体、レジストリおよびその利害関係者の為の国際組織であるDNSOARC会議の正会員。 カリフォルニア大学バークレイ校ハースビジネススクールにてMBAを取得、ロチェスター大学にて経済およびコンピューター科学の両分野で学士号を取得。