SCIS 2013 The 30th Symposium on Cryptography and Information Security
Kyoto, Japan, Jan. 22- 25, 2013
The Institute of Electronics, Information and Communication Engineers

ワンクリック詐欺を防ぐ手法に関する考察
A Study to Protect Users from Threats such as "One-Click Froud"

唐沢 勇輔* 橋本 正樹* 辻 秀典* 田中 英彦*
Yusuke Karasawa Masaki Hashimoto Hidenori Tsuji Hidehiko Tanaka

あらまし ワンクリック詐欺と呼ばれる不正請求手法が登場して久しいが，国民生活センターや IPA 等への相談件数は一向に減少しておらず，またこうした不正請求画面の駆除サービスなるものも登場している現状をかんがみると，技術的な対策が確立しているとは言い難い．このような PC のデスクトップ上に不正請求画面を表示するようなワンクリック詐欺手法では，HTA 形式のファイルが利用されており，この手法についても技術面での対策が取られていない状況がある．よって本稿では，まず，同じ詐欺的手法であるフィッシング詐欺の対策技術に関する先行研究を整理し，ワンクリック詐欺に対しても有効かどうかを整理する．次に，ワンクリック詐欺に利用される HTA ファイルのサンプルと，正当な目的で作成された HTA ファイルのサンプルを複数比較した結果をもとに，ワンクリック詐欺に利用されるような HTA ファイルの特徴を明らかにする．その上で，HTA 形式のファイルを利用したワンクリック詐欺の技術的対策手法について考察する．

キーワード 個人ユーザ，フィッシング詐欺，ワンクリック詐欺，不正請求

1 はじめに

パソコンをはじめとした ICT 機器やブロードバンドの普及に伴い，一般家庭でもインターネットに接続した情報デバイスを利用することはもはや当たり前になってきた．こうした流れとともに，個人が情報セキュリティのリスクに直面する場面が増えている．また，攻撃者の意図が愉快目的や技術誇示から金銭や情報詐取といった具体的な利益に変化する中で，過去には「ウイルスに感染してパソコンが使えない」といった程度の被害だったものが，「情報を詐取されカードを不正利用される」というより実被害を伴うものに変化しており，リスクの深化が見られる．IT が生活に浸透するようになったことによって，リスクが量的・質的に拡大していると言えよう．

* 情報セキュリティ大学院大学, 〒 221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1
Institute of Information Security, 2-14-1 Tsuruyacho, Kanagawa-ku, Yokohama-shi, Kanagawa, 221-0835, Japan.

個人・家庭での IT 利用者に着目した場合，情報セキュリティ上の脅威は多岐にわたるが，以下の 4 種類に分類できる．

	脅威類型	脅威
a	直接的な金銭被害	ワンクリック詐欺，偽セキュリティソフト
b	情報詐取による金銭被害	マルウェアによる情報詐取，フィッシング詐欺，盗聴
c	情報機器の利便性低下	マルウェア感染，迷惑メール
d	心理的な被害	なりすまし

表１：個人をとりまく脅威の類型

この 4 種類のうち，金銭被害につながるのは a および b だが，この内，不正送金やカードの不正利用についてはサービス提供者による補償が行われることがあるものの[1][2]，一般的には，一度支払ってしまった金銭を取り戻すのは困難である．従って，a

およびｂによる被害を防ぐためには，IT 利用者を保護する方策が必要であるが，ｂについては学術研究・商用製品を問わず広く検討されている一方で，ａのうち，特にワンクリック詐欺については日本特有の事象であるためか，研究例が少なく検討が不十分である．同時に，ａは，IPA への相談件数でみると 2011 年の 1 年間で 5,509 件[3]，国民生活センターや全国の消費者センターへの相談件数でみると 2011 年で 95,545 件[4]に上り，マルウェア感染と比較して現象が目に見えやすいという事実を差し引いてもその相談件数の多さは目を引くものがあり，また，インターネットホットライン連絡協議会に寄せられる相談件数でも，約 23% がワンクリック詐欺等に起因する架空請求にあたる．さらに，これらの相談件数を俯瞰すると，マルウェア等に比べて前年比件数があまり減っていないのもａの特徴として挙げられる．

このような背景のもと，本研究では，最近のワンクリック詐欺に特徴的な HTA ファイルを用いた手法を紹介し，その対策について考察を行うものである．考察にあたっては，ワンクリック詐欺そのものの先行研究が少ないことから，同じ詐欺的手法であるフィッシング詐欺の研究事例をもとに考察を行った．また，実際にワンクリック詐欺に利用されている HTA ファイルを web から収集し，正当な理由で配布されている HTA ファイルと比較することで対策手法を見出せないか検討した．

以降，本稿では，はじめに第 2 章でワンクリック詐欺の特徴を，被害事例や感染経路から説明し，続いて，第 3 章でワンクリック詐欺の先行研究を紹介する．その後，第 4 章と第 5 章で既存のフィッシング詐欺対策の研究をもとにした対策手法の考察を行い，最後に，第 6 章でまとめと今後の課題を述べる．

2　ワンクリック詐欺の特徴

2.1　被害事例からみる特徴

国民生活センターに寄せられた相談事例を見ると，アダルトサイトを経由して被害にあうことが多いが，「パソコンで友人のブログにリンクされた動画を友人の動画だと思い込んで」[4]という事例もある．共通しているのは動画を閲覧しようとしてユーザ自身でクリックをしている点にある．マルウェア感染はドライブバイダウンロード攻撃に代表されるようにいかにユーザに気づかれずに感染させるかが基本的な動機づけとしてあるが，ワンクリック詐欺の場合はクリックという能動的な行動をさせているために，ユーザ自身にも後ろめたさがあり，支払いにつながってしまっているものと考えられる．

2.2　典型的な感染経路

パソコン上にワンクリック詐欺画面を表示させる手法は，HTA ファイルを利用した手法が用いられており，以前からみられる手法であるが未だに変わっていない．典型的な経路は以下のとおりである．[5]

(1) 検索などで問題のサイトを閲覧
(2) 無料動画を再生するよう画像をクリック

図１：典型的な感染経路例１

(3) 利用規約への同意画面をクリック
※このステップで複数回クリックを求められることも多い．

図 2：典型的な感染経路例 2

(4) 動画リンクをクリック
(5) Windows のセキュリティ警告で[開く]や[実行]をクリック

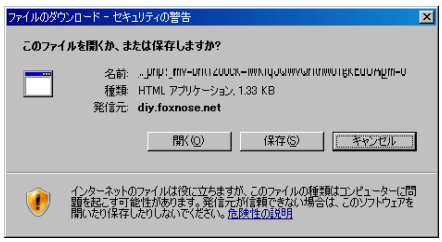

図 3：典型的な感染経路例 3

(6) 手順(5)を実行した結果として，デスクトップ画面に不正請求あるいは登録完了のメッセージが表示され続ける．

図 4：典型的な感染経路例 4

ワンクリック詐欺につながるサイトでは多くの場合その入口で，この手順が詳細に案内されている．ユーザはその指示に盲目的に従って「画面が出続ける」という結果を予測せずにこの手順を進めていると思われる．

手順(6)でパソコンの画面にポップアップを表示させ続ける方法としては 2 種類あり，レジストリのスタートアップ用のパスに URL をパラメータとして mshta.exe を実行するように書き込みパソコン起動時に画面を表示しているものと，Windows のタスクスケジューラに同じく URL をパラメータとして mshta.exe を実行するように登録される方法がある．後者の場合，画面を閉じてもすぐに表示され，被害事例にあるように「パソコンに画面が張り付いて取り除けない」といった状態に陥る．

2.3 HTA ファイルを用いた手法のメリット

パソコンにポップアップ画面を表示させるだけであれば，そうした機能を持つプログラムを作成するなど多くの手法が考えられるが，攻撃者はなぜ HTA ファイルを用いた手法を採用しているのだろうか．トレンドマイクロ社[6]によると本手法には，攻撃者にとっては以下のようなメリットがある．

- EXE ファイルよりユーザの警戒感が低い．
- HTA の中で転送させるため，ダウンロードファイルのソースだけではレジストリを改変させる悪質なコードを確認出来ない．
- 転送先の HTML には，暗号化された VBScript を使用し，人の目では動作が判別できないようにしている．
- 「mshta.exe」を利用し，警告を出す事無くスクリプトコードを実行させている．

これらに私見を加えると，技術的には単純で流用が容易な手法であるため，技術的な成熟度が低くても攻撃を成功させられることにあるのではないかと考える．HTA ファイルを用いたワンクリック詐欺の手法が世の中に現れてから，現在に至るまで技術的には大きな変化が見られないことも，このことを証明しているのではないか．

3 ワンクリック詐欺対策の先行研究

ワンクリック詐欺（不正請求）についての学術研究は，日本特有の現象であるためか，海外においては研究自体が少ない．国内の研究では，名越らによって，web ページ中の単語情報を用いてワンクリック詐欺を防止する手法[7]が提案されている．

この手法は，詐欺的ページにみられる特有の単語を複数抽出して，その発言割合によって詐欺ページ

か非詐欺ページ（正常ページ）かを判定するものである．実際のワンクリック詐欺ページを用いて実験を行ったところ詐欺ページの的中率が 95%，非詐欺ページの判別的中率が 94%と比較的高い精度で判別を行うことができている．

しかしながら，本研究の提案手法では web ブラウザで表示される請求画面に対しての判定しか行えないため，HTA ファイルを用いてウィンドウ内に請求画面を表示するような手法については有効ではないと考えられる．

そのほかの，ワンクリック詐欺に対抗することを目的にした研究でも web ブラウザ上で表示される請求画面を解析したり，あるいはブラックリスト化してブロックしたりといった研究が多い([8][9][10])．市場においては，駆除サービス([11])なるものがセキュリティ各社から提供されているが，これは一方で技術的な対策が確立していないことを示しているともいえよう．

4　先行研究としてのフィッシング詐欺対策

4.1　フィッシング詐欺対策の分類

フィッシング詐欺を技術的に防ぐ手法については，国内外で多くの研究がある．本節では，同じ詐欺的手法であるフィッシング詐欺をユーザ側で技術的に防ぐことを提案したいくつかの研究を整理することで，ワンクリック詐欺に利用できるものがないか考察したい．なお，ここではフィッシング詐欺を誘導するメールを防ぐような手法は対象から除外している．HTA ファイルを用いたワンクリック詐欺については，メールから誘導されるという事例は知られていないためである．

フィッシング詐欺をユーザ側で防ぐ手法は，(1) URL データベースを利用するもの，(2)web ページに表示されるコンテンツ情報を利用するもの，(3)HTTP リクエストの特徴を利用するものの３つに大別できる．(1)の手法の代表的なものは商用サービスとして一般的なブラックリスト方式である．ブラウザのプラグインやアプライアンスとして，有償・無償を問わず市場において多くの製品が提供されている．ブラックリスト・ホワイトリストのデータベースの優劣によって効果の高低が変わってくるものである．学術研究としては，ソーシャルブックマークを URL 評価に用いる手法[12]が提案されているたり，事前にユーザ固有のホワイトリストを用意してフィッシングサイト判定をより確実に行えるようにした手法[13]などがある．

(2)は，フィッシングサイトに特徴的なページコンテンツをもとにフィッシングサイト判定を行うものである．たとえば，フィッシングサイトが正規サイトの模倣であることに着目し，当該ページから企業名を抽出して企業名に対応する正規 URL ホワイトリストと当該ページ URL を比較して判定する手法[14]や，当該ページから自然言語処理と統計分析によって抽出したキーワードをもとに検索エンジンで正規サイトを見つけ当該ページと比較する手法[15]などがある．コンテンツという大きくは変化しにくい特徴点に着目して判定することで，ブラックリスト方式における「後追い」という課題を解決し，より汎用的な対策を目指したものである．

(3)については，フィッシングサイトの存続期間が短いという特徴に着目し，ドメイン名や個人情報の詐取といった７つの特徴をもとに判定する[16]がある．(2)同様，データベースに依存せず汎用的にフィッシングサイトの判定を行なうことを目指したものである．コンテンツのみならず web サイトの存続期間などの情報を判定材料にしているという点と，プロキシサーバーでの実装を提案している点が特徴的である．

4.2　ワンクリック詐欺対策への応用

(1)の手法については，ワンクリック詐欺につながる HTA ファイルをダウンロードするサイトの URL をブラックリスト化し，そのデータベースをもとにサイトへのアクセスやファイルダウンロードをブロックするという手法が考えられる．しかし，フィッシング詐欺対策と同様に，ブラックリストに存在していないサイトについてはブロックされないという課題は残る．あるいは，ソーシャルブックマークの考え方を応用し，アクセス数が著しく少ない URL につ

	Site	Domain	IP address	Country	Date first seen
良性					
1	http://saigae.jp	qae.jp	202.181.98.166	JP	Aug-05
2	http://saigae.jp	qae.jp	202.181.98.166	JP	Aug-05
3	http://saigae.jp	qae.jp	202.181.98.166	JP	Aug-05
4	http://saigae.jp	qae.jp	202.181.98.166	JP	Aug-05
5	http://saigae.jp	qae.jp	202.181.98.166	JP	Aug-05
6	http://saigae.jp	qae.jp	202.181.98.166	JP	Aug-05
7	http://saigae.jp	qae.jp	202.181.98.166	JP	Aug-05
8	http://saigae.jp	qae.jp	202.181.98.166	JP	Aug-05
9	http://www.microsoft.com	microsoft.com	64.4.11.42	US	Aug-95
10	http://crocro.com	crocro.com	124.146.200.136	JP	May-08
11	http://q.hatena.ne.jp	hatena.ne.jp	59.106.194.44	JP	Feb-08
12	http://tuka.s12.xrea.com	xrea.com	203.189.104.112	JP	Mar-06
13	http://www.sn.rim.or.jp	rim.or.jp	202.247.191.227	JP	Aug-96
14	http://www.vector.co.jp	vector.co.jp	203.191.227.53	JP	Jan-96
15	http://www4.airnet.ne.jp	airnet.ne.jp	210.159.71.45	JP	Oct-98
悪性					
1	http://div.foxnose.net	foxnose.net	100.42.236.170	US	unknown
2	http://vdr.becauseon.info	becauseon.info	100.42.236.169	US	unknown
3	http://gnf.onjdisljsjewq.net	onjdisljsjewq.net	61.115.127.203	JP	unknown
4	http://gfs.m.degfnujdq.net	m.degfnujdq.net	61.115.127.203	JP	unknown
5	http://jum.fekoe.net	fekoe.net	61.115.75.45	JP	unknown
6	http://isw.ktmsh.net	ktmsh.net	61.205.55.43	JP	unknown
7	http://bdo.aihs.net	aihs.net	61.205.55.43	JP	unknown
8	http://nva.hsom.r.net	hsom.r.net	61.205.55.43	JP	unknown
9	http://bdo.qepon.net	qepon.net	61.205.55.43	JP	unknown
10	http://x1w.answerin.info	answerin.info	64.62.177.164	US	unknown
11	http://bib.answerin.info	answerin.info	64.62.177.163	US	unknown
12	http://ry8.answerin.info	answerin.info	64.62.177.167	US	unknown
13	http://vvt.quicklyto.info	quicklyto.info	100.42.236.169	US	Jan-13
14	http://6z2.traightest.info	traightest.info	100.42.236.174	US	unknown
15	http://xuf.traightest.info	traightest.info	100.42.236.172	US	unknown
16	http://bac.traightest.info	traightest.info	100.42.236.174	US	unknown
17	http://fv7.sadkind.info	sadkind.info	100.42.236.169	US	unknown
18	http://fv7.sadkind.info	sadkind.info	100.42.236.174	US	unknown
19	http://4ne.sadkind.info	sadkind.info	100.42.236.170	US	unknown
20	http://www.leavescup.info	leavescup.info	100.42.236.169	US	unknown
21	http://e1s.leavescup.info	leavescup.info	100.42.236.173	US	unknown
22	http://bu3.leavescup.info	leavescup.info	100.42.236.172	US	unknown
23	http://brh.leavescup.info	leavescup.info	100.42.236.171	US	unknown
24	http://g3z.hawknailcom	hawknailcom	100.42.236.169	US	unknown
25	http://umm.hawknailcom	hawknailcom	100.42.236.173	US	unknown
26	http://3j7.hawknailcom	hawknailcom	100.42.236.171	US	unknown
27	http://nhd.bsjz.org	bsjz.org	61.115.121.238	JP	unknown
28	http://fk.abkfd.org	abkfd.org	61.115.121.238	JP	unknown
29	http://dqc.abkfd.org	abkfd.org	61.115.121.238	JP	unknown
30	http://punctatus.nukisute.info	nukisute.info	65.49.39.119	US	unknown

表 2：HTA ファイルのダウンロード URL 解析

いてはブロックするという手法も考えられるがこの場合は誤検出が課題になるであろう．

(2)の手法については，ワンクリック詐欺の場合，正規サイトのようなものが存在するわけではないため，[14][15]のような手法をとることは難しい．コンテンツにおける特徴点を何らかの形で抽出してワンクリック詐欺サイトとして判定する[7]のようなアプローチは考えられるが，HTA ファイルをダウンロードする手法の中には，被害事例でも示した通り友人のアップロードした動画と錯誤して閲覧（HTA ファイルのダウンロードと実行）を行ってしまうようなケースも見られるので，こうしたケースに対す

る有効性は疑問が残る．

(3)については，ワンクリック詐欺に利用されるHTAファイルをダウンロードするページのURLも，フィッシングURL同様に存続期間は短いと考えられる．フィッシング詐欺同様，ワンクリック詐欺のサイトもブラックリストによる検知を回避するために日々新しいURLが生まれているためである．誤検出の可能性を低くするため，HTAファイルのダウンロード元URLの存続期間等の特徴から判定を行うということも考えられよう．また，ワンクリック詐欺のポップアップウィンドウはブラウザ内に表示されるわけではないので，ポップアップウィンドウを経由して行われている通信を解析して判定するという手法を想定した場合，ブラウザに依拠しないプロキシを利用する手法については参考になると思われる．

5　悪性HTAファイルと良性HTAファイル

ここでは，便宜的にワンクリック詐欺の過程で実行されるHTAファイルを「悪性HTAファイル」，正規の目的で利用されるHTAファイルを「良性HTAファイル」と呼称する．悪性ファイルはワンクリック詐欺に利用されているサイトを検索し，実際にダウンロードされるHTAファイルを収集したものである．すべてのファイルでパソコン内にポップアップ画面を表示させる動作を行うことを確認している．良性ファイルについては，スクリプトファイルやサンプルスクリプトを提供している複数のサイトからダウンロードしたHTAファイルである．こちらも実際に実行して動作に問題ないことを確認している．

ここで，ワンクリック詐欺は論理的には2.2で示した感染経路のいずれのステップでも防ぎうるわけであるが，手順(6)でポップアップ画面しまう問題も防止することを主眼におきたい．たとえば，ポップアップ画面内に表示される内容を解析して詐欺であるという結果を示してもワンクリック詐欺自体は防げるが，パソコンのデスクトップに表示されるポップアップそれ自体もユーザにとっては迷惑なものに変わりないためである．そこで，HTAファイルそれ自体を比較するよりは，悪性HTAファイルと良性HTAファイルをダウンロードする元URLに着目して，Netcraftから得られる結果の比較を行った．詳細は表２の通りである．

良性15サンプル，悪性30サンプルに対する結果であるが，悪性HTAファイルのダウンロードもとについてはほとんどがサイト立ち上げ日が不明であることがわかる．一方で，経験的に知られている，サイト提供サーバが国外にあるという点については，必ずしもすべてのURLが国外とは言えないことも見て取れる．

検討対象としたサンプルが少ない状況ではあるが，HTAファイルのダウンロード元URLに着目した場合，悪性と良性では明らかな差があると言えるのではないか．

6　まとめと今後の課題

本稿では，いまだに被害の減らないワンクリック詐欺を，ユーザ環境において技術的に防ぐことを目的に，同じ詐欺的手法であるフィッシング詐欺を防ぐ手法を参考に考察を行った．その結果，悪性HTAファイルのダウンロード元URLはフィッシング詐欺サイト同様，存続期間が短いという特徴を見出すことができた．

一方で，この１点の特徴点のみで判断してしまうと，個人サーバや新たに作成されたサイトからダウンロードされる良性HTAファイルを誤検知してしまうという問題が発生しうる．そのため，判定に併用することができる特徴点を見出す必要がある．

参考文献

[1] http://www.jabank.org/osirase/080901a.html (2012/12/12確認)

[2] http://www.cr.mufg.jp/member/service/basic/use/security/approach/amends/index.html (2012/12/12確認)

[3] インターネットホットライン連絡協議会「2012（平成24）年メール相談項目月別件数」http://www.iajapan.org/hotline/data/data.html

[4]国民生活センター報道発表資料 http://www.kokusen.go.jp/pdf/n-20120906_1.pdf

[5] IPA注意喚起「第11-01-132-4号」http://www.ipa.go.jp/security/topics/alert20080909

.html
[6]トレンドマイクロ セキュリティ ブログ「HTA を利用したワンクリックウエアの新たな手口」
http://blog.trendmicro.co.jp/archives/2729
[7] 名越潤也, 田中英彦, 単語情報を用いたワンクリック詐欺対策手法の提案, 2007 年暗号と情報セキュリティシンポジウム(SCIS2007), 2007 年.
[8] 高正博, 畑上英毅, ソーシャルエンジニアリング攻撃の分析と対策, 紀要開発工学部／第18号(2008), 2008年
[9] 柴田賢介, 神谷造, 佐野和利, 荒金陽助, 塩野入理, 金井敦, 迷惑メールにおける誘導手法に関する一考察, 情報処理学会研究報告(2007-CSEC-38), 2007 年.
[10] 松木隆宏, 新井悠, URL ブラックリストの効率的な利用方法の一検討, 電子情報通信学会 信学技報(ICSS2009-12), 2009 年.
[11] トレンドマイクロ社「おまかせ！不正請求クリーンナップサービス」
http://safe.trendmicro.jp/products/popupcleanup.aspx
マカフィー社「ウイルス駆除サービス」
http://www.mcafee.com/japan/home/vrs/
[12]中山心太「ソーシャルブックマークを用いたフィッシング検知技術」(2009-FI-94(5))
[13] A. Belabed, E. Aimeur, A. Chikh "A personalized whitelist approach for phishing webpage detection" (2012 Seventh International Conference on Availability, Reliability and Security)
[14] 柴田賢介, 荒金陽助, 塩野入理, 金井敦「Web サイトからの企業名抽出によるフィッシング対策手法の提案」(2006-DPS-128(4))
[15] 中山心太, 吉浦裕「模倣コンテンツの特性に基づくフィッシング検知方式」(2007-CSEC-38(57))
[16] 中村元彦, 寺田真敏, 千葉雄司, 土居範久「プロキシを利用した HTTP リクエスト解析によるフィッシングサイト検出システムの提案」(情報処理学会論文 Vol.48 No.10)