社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2006－EIP－31（5）
2006／3／18

フィッシング詐欺の状況と対策に関する考察

荒金 陽助† 間形 文彦† 柴田 賢介† 塩野入 理† 金井 敦†

† 日本電信電話株式会社，NTT 情報流通プラットフォーム研究所

あらまし 金融機関の顧客などをターゲットとし，巧みな文言をちりばめたメールで偽サイトに被害者を誘導し，クレジットカード番号や口座番号，暗証番号などを盗み取るフィッシング詐欺が日本でも発生し始めている．本論文では，フィッシング詐欺について典型例を示し，法的・技術的観点からその現状を議論した．日本の現行刑法においては，有体物ではない “情報” を騙し取られたことに対して詐欺罪は適用されず，フィッシング詐欺の被害者を救済することは困難であることを示す．また，技術的に洗練度を増すフィッシング詐欺に対して，代表的な対策である，サーバ証明方式およびブラックリスト方式について説明し，その課題について議論する．

キーワード フィッシング詐欺，ネットワーク犯罪，金融機関，著作権法，刑法，不正アクセス禁止法

A Study of Phishing Attacks' Trends and Solutions

Yosuke Aragane† Fumihiko Magata† Kensuke Shibata†
Osamu Shionoiri† Atsushi Kanai†

† NTT Information Sharing Platform Laboratories, NTT Corporation

Abstract Phishing is a network fraud to theft important personal data such as credit card number, password or social security number etc. In this paper, we discuss about the phishing in the law and technical point of view. Since the existing criminal law could not punish the information theft, it is difficult to relieve a victim of phishing fraud. On th other hand, we discuss about some anti-phishing solutions such as server certificate and URL black list approaches.

Keywords Phishing, Network Crime, Copy Right Law, Criminal Law, Unauthorized Computer Access Law

1 はじめに

最近，振り込め詐欺（オレオレ詐欺）の IT 版的な詐欺手法とも言える，フィッシング詐欺という犯罪が新聞などでも散見されるようになってきた．その特徴は，発信者や内容を偽装した電子メールを用いて被害者を “釣る” ことを発端として，ソーシャルエンジニアリング[1]や技術的な偽装によって，クレジットカードなどの重要な情報を盗み取る詐欺であるといわれている [2]．

クレジットカード情報や社会保障番号（Social Security Number）の騙取を狙ったフィッシング詐欺は，以前より欧米では著名な犯罪となっていたが，日本での犯罪例はほんとんど見られなかった．日本では欧米と比してクレジットカードの普及率が低いことと，フィッシング詐欺ではフィッシングメールの文面やフィッシングサイトのデザインに，被害者を騙すための高度な言語能力が必要なため，日本語という言語の壁が欧米のフィッシング詐欺師にとって文字通り障壁となっていた可能性がある．しかしながら，インターネットオークションやオンラインバンキングの普及に伴い，それらのサービスのアカウント情報を狙ったフィッシングが日本でも続発するようになってきた．フィッシング詐欺の存在や手法が有名となったことによる，日本人のフィッシング詐欺師の出現が大きな原因と考えられる．また，偽装対象企業のロゴ画像などフィッシングに必要な情報一式を格納したフィッシング CD-ROM が欧米のブラックマーケットで流通するようになったことも無関係ではないと思われる．

欧米においては，フィッシング詐欺によってオンラインバンキングの閉鎖例も報告されるなど，その社会的・金銭的被害は看過できない状況になってきている．フィッシング詐欺はソーシャルエンジニアリングを駆使

[1] ソーシャルエンジニアリング（Social Engineering）：社会の仕組みや人間関係を操り，騙しと誘導と説得の技術を駆使して情報を盗むこと [1]．

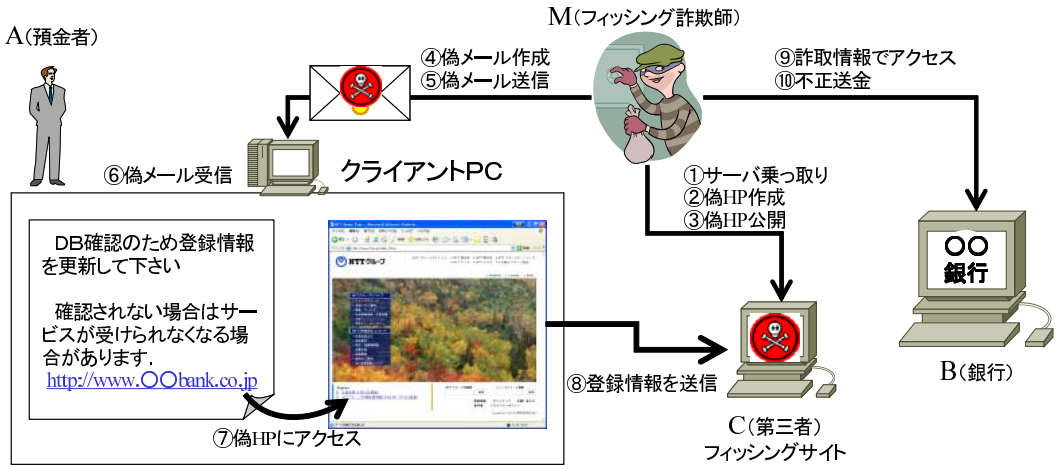

図 1: 典型的なフィッシング詐欺の流れ

する犯罪であり，その防止のためには，技術的な防止策のみならず，法的な抑止策についても十分に検討することが必要であろう．我が国では警察庁がフィッシングおよびフィッシング詐欺を以下のように定義するとともに [3]，フィッシング詐欺に対する警告が広報されている．

「フィッシングとは、銀行等の企業からのメールを装い，メールの受信者に偽のホームページにアクセスするよう仕向け，そのページにおいて個人の金融情報（クレジット番号，ＩＤ，パスワード等）を入力させるなどして個人の金融情報を不正に入手するような行為をいう．その情報を元に金銭を騙し取る手口がフィッシング詐欺といわれる.」

しかし，フィッシング詐欺に対する技術的対策と比較して，法的・技術的なカバー領域などの議論はほとんどなされていない．そこで本論文では，フィッシング詐欺について概観した後に，法的および技術的観点で見たフィッシング詐欺及び対策について議論する．

2　フィッシング詐欺の特徴

本章ではフィッシング詐欺の特徴とその典型的な流れについて説明する．

2.1　統計的特徴

フィッシング詐欺について様々な観点で調査を行っている Anti-Phishing Working Group (APWG) のレポートの概要を表 1 に示す．

フィッシング詐欺がオンライン詐欺である特徴として，フィッシングサイトの短寿命化が挙げられる．2004 年の 10 月には 6.4 日であったフィッシングサイトの平均寿命が，約一年で 5.3 日と約一日縮まっており，フィッシング詐欺の短期決戦化が進んでいると考えられる．これと関係して，新しくオンラインとなるフィッシングサイトの数も激増し，同じく 2004 年の 10 月には 1142 サイト/月であったものが，約一年で 7197 と 6 倍以上の伸びとなっている．2005 年 12 月には，単純計算で毎日 232 のフィッシングサイトが新しく立ち上がっていたことになる．また，膨大な会員を抱える金融機関などをターゲットとすることで，効率的なフィッシング詐欺が可能となることから，6,7 個の巨大ブランドをターゲットとするフィッシング詐欺が多数（8 割以上）である状況は変化がない．

2.2　典型例

インターネットバンキングを対象とした典型的なフィッシング詐欺の流れを図 1 に示し，そのプロセスを説明する．犯人を M，預金者 A，銀行 B，第三者 C とする．

① M は C の Web サーバの脆弱性等を利用して侵入し，自己の支配下に治める．

② M は B の本物の Home Page (HP) に類似する偽 HP を作成する．偽 HP には「登録情報の更新」を求める記載がある．

③ M はインターネットに接続された C の Web サーバ上で偽 HP を公開する．

④ M は偽 HP へのアクセスを誘引するメールを作成する．メールには「登録情報の更新」を求める記載がある．

表 1: APWG レポートの概要

contents	value
Number of unique phishing sites received in December	7197
Number of brands hijacked by phishing campaigns in December	121
Number of brands comprising the top 80% of phishing campaigns in December	7
Country hosting the most phishing websites in December	United States
Contain some form of target name in URL	51%
No hostname just IP address	32 %
Percentage of sites not using port 80	7%
Average time online for site	5.3 days
Longest time online for site	31 days

⑤ M は B を送信元と偽ったメールを特定多数または不特定多数の第三者（A を含む）に大量送信する．

⑥ A は自己あてのメールを受信する．

⑦ A は受信したメールの記載内容を信じてその指示に従い偽 HP にアクセスする．

⑧ A は偽 HP の記載内容を信じて ID，パスワード等の A の個人情報を偽 HP に自ら入力する．

⑨ M は B のインターネットバンキング HP にアクセスし，A の ID，パスワード等をシステムに入力する．

⑩ B は A になりすまし，A の口座から預金を M の管理下にある他の口座等へ送金する．

また，このプロセスを一覧化したものを表 2 に示す．以下，表 2 にしたがって，法的・技術的に各プロセスを分析する．

3 犯罪類型と法適用

本章では，日本の現行刑法におけるフィッシング詐欺の犯罪類型と法適用，今後の法的課題について考察する．

3.1 フィッシング詐欺と犯罪類型

フィッシングの何がどの犯罪に該当するかを検討するため，2.2 節で示したインターネットバンキングのフィッシング詐欺を例に議論する．

3.1.1 「詐欺」の被害者は誰か

2.2 節で示したプロセスから，誰がどの時点で「詐欺」に遭い，何を騙し取られたのであろうか．詐欺とは人を欺網して錯誤に陥れ，財物を騙取したり瑕疵ある意思表示を行わせることをいう [4]．⑦において A が偽メールを本物と錯誤し，かつ「登録情報更新」が必要であると錯誤して偽 HP にアクセスしたことは明らかである．しかし，⑦では偽 HP にアクセスしたのみであり，この時点で何かを騙し取られたとはいえない．一方，⑧において A はアカウントの確認等をするため ID，パスワード等を入力する．ID，パスワード等は「財物」に該当するであろうか．刑法上の「財物」とは有体物を指すとされ，ID，パスワード等の情報は無体物であり「財物」には当たらない．したがって，⑧においても詐欺の構成要件を満たさず，詐欺罪（刑法 246 条）は成立しないのである．

ならば⑩はどうか．M は A の預金口座から M の管理下にある他の口座へ不正に送金し，現金を騙し取っている．電子計算機使用詐欺罪（刑法 246 条の 2）の構成要件を満たす可能性が高い．M の行為はインターネットバンキングシステム，すなわち電子計算機に「虚偽の情報」を与えて,「財産上不法の利益を得」た場合に当たるからである．このとき法上の被害者は電子計算機を使用管理する B であって，A ではない．したがって，自己の口座から預金を引き出されたにも係らず，A は被害届けを直接警察に提出することはできない．なお，A と B との関係については民法の債権の準占有者に対する弁済（民法 478 条）等が論点になるが刑事問題を扱う本稿では論じない．

現行刑法においてこの例のフィッシング詐欺の被害者は A ではなく B であり，M の A に対する行為は詐欺等の犯罪類型に該当しないのである．

3.1.2 不正アクセス行為

詐欺等以外に適用可能な犯罪類型として不正アクセス行為がある．

⑨において M は A の ID とパスワードを B のインターネットバンキングシステムに入力している．この行為はアクセス制御機能を有する特定電子計算機に電気通信回線を通じて，他人の識別符号を無断で入力す

表 2: フィッシング詐欺のプロセスと犯罪類型，それに対応する技術的対策

分類		行為の主体	フィッシング詐欺のプロセス		適用可能性のある犯罪類型	法上の被害者(告訴できる者)	実益上の被害者	M の技術的手口	技術的対策 主体	技術的対策 手段
フィッシング詐欺	フィッシング	M	①	M が C の Web サーバを乗っ取り	不正アクセス行為（不正アクセス禁止法 3 条 2 項 2 号，3 号）	C	C		C	サーバセキュリティ対策
			②	M が偽 HP を作成	複製権の侵害（著作権法 119 条）	B	B	※ 1	B	すかし
			③	M が偽 HP を公開	送信可能化権の侵害（著作権法 119 条）	B	B			
			④	M が偽メールを作成	複製権の侵害（著作権法 119 条）	B	B	※ 2		
			⑤	M が偽メールを大量送信	行政命令違反（特定電子メール適正化法 18 条）ただし，ほぼ適用はあり得ない.	(主務大臣)	サービスプロバイダ等		サービスプロバイダ等	フィルタリング
		A	⑥	A が偽メールを受信 =M が偽メールの送信に成功	なし	なし	A		A	スパムメールフィルタ
			⑦	A が偽 HP へアクセス =M が A の誘引に成功	なし	なし	A	効果としての※ 2	A	サーバ証明書，ブラックリスト
			⑧	A が偽 HP への個人情報を入力 = M が A の個人情報の騙取に成功	なし	なし	A	効果としての※ 1	A	個人情報フィルタ
		M	⑨	M が騙取した個人情報による B へのアクセス	不正アクセス行為（不正アクセス禁止法 3 条 2 項 1 号）	B	A,B	マンインザミドル攻撃	B	ワンタイムパスワード
			⑩	M が金銭等を騙取	電気計算機使用詐欺 (刑法 246 条の 3)，電磁的記録不正作出・供用 (刑法 161 条の 2 第 1 項，第 3 項)	B	A,B			
			②，④		電磁的記録不正作出（刑法 161 条の 2 第 1 項）ただし、偽メール・偽 HP が「権利、義務又は事実証明」に関する場合のみ	A	A,B,C			
			③，⑤～⑦		電磁的記録不正供用（刑法 161 条の 2 第 3 項）ただし、偽メール・偽 HP が「権利、義務又は事実証明」に関する場合のみ	A	A,B,C			
			①～③，⑤，⑨，⑩		電子計算機損壊等業務妨害（刑法 234 条の 2）. ただし, 故意の立証が困難	C，B，サービスプロバイダ等	C，B，サービスプロバイダ等			
			① ～ ⑩		偽計業務妨害（刑法 233 条後段）威力業務妨害（刑法 234 条）. ただし，故意の立証が困難	A, B, C, サービスプロバイダ等	A, B, C, サービスプロバイダ等			

※ 1 ロゴ，自己署名証明書，アドレスバー偽装，フレーム乗っ取り，※ 2 ロゴ，HTML メール

る行為（不正アクセス禁止法 3 条 2 項 1 号）に該当する.「アクセス制御機能」とは，特定電子計算機の特定利用を自動的に制御するために当該特定利用に係るアクセス管理者によって当該特定電子計算機又は当該特定電子計算機に電気通信回線を介して接続された他の特定電子計算機に付加されている機能であって，当該特定利用をしようとする者により当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号であることを確認して，当該特定利用の制限の全部又は一部を解除するものをいう（同法 2 条 3 項）. 電気通信回線とはインターネット等を指す．識別符号とは「当該アクセス管理者によってその内容をみだりに第三者に知らせてはならないものとされている符号」（同法 2 条 2 項 1 号）をいい，ここではパスワードや ID が該当する．したがって，M の⑨の行為は不正アクセス行為として罰則の適用を受けることがある（同法 8 条 1 号）．このとき法上の被害者は「特定電子計算機」たるインターネットバンキングシステムを管理する B であって，A ではない．その点で電子計算機使用詐欺罪と同様である.

同様に①の M による C の Web サーバの乗っ取りも不正アクセス行為に該当する可能性が高い．①の行為はアクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く.）又は指令を入力して当該特定電子計算機を作動させ，その制限されている特定利用をし得る状態にさせる行為（不正アクセス禁止法 3 条 2 項 2 号）に当たる.「特定利用」とは電気通信回線に接続している電子計算機の利用（同

法 2 条 1 項）をいう．すなわち，正しい ID やパスワードに依らずに，Web サーバの脆弱性等を突いてアクセス制御を免れ，その Web サーバを利用可能とする行為を指す．このとき法上の被害者は Web サーバを管理する C である．

3.1.3 著作権の侵害

著作権の侵害行為も刑罰の対象となる．刑法は,「他の法令の罪に対する適用」（刑法 8 条）がされるからである．

②M は B の偽 HP を作成し，③インターネットで公開している．②の行為は著作権のうち複製権（著作権法 21 条）の侵害に該当する可能性が高い．B の HP が B の著作物に該当するとき，B はその著作物を複製する権利を占有する．すなわち，B はその意思に依らずに B の著作物を他人に複製されない権利を持つ．また④メールを作成する行為は，メールの記載に B の HP の著作物の一部の添付等によって，メールに B の著作物性が認められるとき，②と同様に複製権の侵害となることがある．

さらに B はその著作物を自動公衆送信する権利を占有する（著作権法 23 条）．自動公衆送信とは公衆からの求めに応じ自動的に行う公衆送信をいう（著作権法 2 条 1 項 9 号の 4）．公衆送信とは公衆によって直接受信されることを目的として行う送信である（著作権法 2 条 1 項 7 号の 2）．インターネット上の Web サーバによる HP の公開等がこれに当たる．著作権法は自動公衆送信の準備行為も著作者の権利として規定する．すなわち，HP のコンテンツをインターネットに接続された Web サーバにアップロードする行為（著作権法 2 条 1 項 9 号の 5 イ）ならびに HP のコンテンツが入力された Web サーバをインターネットに接続する行為（著作権法 2 条 1 項 9 号の 5 ロ）である．これらを送信可能化という．M は③において B の送信可能化権を侵害している．⑦のアクセスが成功して A に偽 HP が送信された段階で自動公衆送信が成立するが，著作権法は③の送信可能化の段階で権利侵害を認めるのである．

したがって，M は②③④において B の複製権，送信可能化権の侵害罪（著作権法 119 条）の適用を受けることがある．

3.1.4 その他の犯罪類型

以上の他にも僅かだが適用可能性のある犯罪類型がある．

⑤における大量のメール送信は，いわゆるスパムメールに該当する．これはインターネットを運用するサービスプロバイダ等の通信設備に過大な負荷を与える．スパムメールは,「特定電子メールの送信の適正化等に関する法律」による特定電子メールとして規制を受けることがある．同法が定める一定の表示義務等（同法 3 条）に従わない者に対して，総務大臣は必要な措置命令をすることができ（同法 6 条），命令に違反するときは罰金刑（同法 18 条）を科すことができる．直罰制ではなく，行政刑罰である．しかし，同法の対象となるのは「自己又は他人の営業につき広告又は宣伝を行うための手段として送信をする電子メール」（同法 2 条 2 項）であるから，フィッシング詐欺を目的とするメールが，他人 B の営業の広告又は宣伝を行う手段を兼ねることは稀であり，また M が行政命令を受けることは現実的にはほぼありえないと考えられる．

⑩について，M は B の「事務処理を誤らせる目的で，その事務処理の用に供する権利，義務又は事実証明に関する電磁的記録を不正に作った者」（刑法 161 条の 2 第 1 項），それを B の「事務処理の用に供した者」（同条 3 項）に該当し，電磁的記録不正作出・供用罪の適用が考えられる．M は A の口座から不正送金する指示を作成し，B のインターネットバンキングシステムに入力しているからである．預金に係る B の事務処理を誤らせる目的であるから，このときの法上の被害者は B である．また，②④の偽メール・偽 HP の作成を A の事務処理を誤らせる目的と捉えるとき，これを電磁的記録不正作出罪（刑法 161 条の 2 第 1 項），③⑤～⑦を偽メール・偽 HP の供用と捉えるとき，これを電磁的記録不正供用罪（刑法 161 条の 2 第 3 項）が成立すると考えられなくもない．しかし，同罪の成立要件の一つは，電磁的記録が「権利，義務又は事実証明」に該当することである.「登録情報の更新」を求めるだけの偽メール・偽 HP であれば,「権利，義務又は事実証明」に当たるとは考えにくい．同罪の適用は困難であろう．

①～⑩の行為全体を通して，偽計業務妨害罪（刑法 233 条後段）または威力業務妨害罪（刑法 234 条）として法律構成することも考えられる．偽計業務妨害とは偽計を用いて他人の業務を妨害することをいい，威力業務妨害とは威力を用いて他人の業務を妨害することをいう．また，プロバイダのメールサーバに大量のメールを送信することがメールサーバの「使用目的に沿うべき動作をさせず」プロバイダの業務妨害に当たるとき，また①～③，⑨⑩もそれぞれ C，B の Web サーバの「使用目的に沿うべき動作をさせず」C，B の業務を妨害するとき，こうした行為が電子計算機損壊等業務

妨害罪（刑法 234 条の 2）を構成することが考えられる．しかし，A，B，C，プロバイダ等に対する M の業務妨害の故意を立証するのは容易ではない．フィッシング詐欺の場合，M の主な意図が金銭の騙取にあることが多いためである．「罪を犯す意思がない行為は，罰しない」（刑法 38 条）のが刑法の原則である．したがって，業務妨害罪の適用はフィッシング詐欺の場合，困難であろう．なお，同罪が適用されるときの妨害の対象となる業務は B，C，プロバイダ等の業務はもちろん，A の業務として構成することも不可能ではない．業務とは反復継続して行う行為と解されるからである．

表 2 に示すように，A は実益上の被害を受けているにもかかわらず，刑事上は被害者とされることがほとんどなく，事実上，告訴する権利を持つことがない（民事上の A の救済は別にあり得るが本稿では論じない）．

3.2 法適用の実際

わが国における「フィッシング」と「フィッシング詐欺」が初摘発された事件から法適用の実際を検討する．

3.2.1 わが国初の「フィッシング」事件

「フィッシング」がわが国で初めて摘発された事件は 2005 年 6 月 14 日の「偽ヤフー」事件である．インターネット上に開設したヤフーの偽サイトで個人情報を盗み取ったとされ，容疑者は著作権法違反と不正アクセス禁止法違反の罪で起訴された．起訴状などによると，パソコンでヤフーの偽サイトを作り，ネット上に公開して著作権を侵害．偽サイトにアクセスした人からパスワードなどを不正に入手し，ヤフーの会員向けのサービスにアクセスしたとされる [5].

この事件では，②③⑦～⑨と同様の行為が認められる．⑦に該当する行為は検索エンジンに「Yafoo」と誤入力する行為である．⑩に該当する行為はなかったとされ，電子計算機使用詐欺等は適用されていない．したがって，著作権侵害と不正アクセス禁止法違反の容疑により起訴されたものと思われる．

3.2.2 わが国初の「フィッシング詐欺」事件

2006 年 2 月 7 日「フィッシング詐欺」がわが国で初めて摘発された．うそのメールなどで個人のパスワードなどを不正に入手する「フィッシング」でインターネットオークションを舞台に詐欺をしていたとして，警視庁は容疑者を不正アクセス禁止法違反と詐欺の疑いで逮捕した．ヤフーオークションの利用者にうそのメールを送りつけて，ID やパスワードを不正入手，ID などを使い，オークションに出品されていた旅行券などを騙し取ったとされる [6].

報道からは手口の詳細は明らかではないが，この事件では④ ～ ⑨と同様の行為があったものと思われる．また被害者が容疑者に意思表示のできるオークションが犯罪の舞台であることから，容疑者がオークションシステムを通じて、被害者を欺網し錯誤に陥らせた容疑と思われる．したがって，⑩については電子計算機使用詐欺ではなく通常の詐欺により摘発されたものであろう．この事件の場合、詐欺の被害者は A であり，B（ヤフー）ではない．

3.3 今後の課題（情報詐欺・窃盗の刑罰化）

以上，⑥～⑧の行為を取り締まる法規制，犯罪類型がないため，フィッシングは，その他のプロセスにおける犯罪類型の適用により摘発・起訴されていることが明らかとなった．これは情報を騙し取る行為そのものを罰することができないための苦肉の策と映る．こうした不都合を改めるべく，情報窃盗の刑罰化を求める意見がある [7].

「他人の財物を窃取した者は，窃盗の罪」（刑法 235 条）とされる．詐欺（刑法 246 条）と同じく，「財物」とは有体物を指し，無体物である情報は「財物」には当たらない．よって，現行刑法に情報窃盗はあり得ない．

現行の個人情報保護法においても，情報の漏洩行為そのものが罰せられるわけではなく，情報漏洩につながるような安全管理措置義務違反が罰せられるのみである．すなわち，義務違反がなければ罰することはできない．しかも，直罰制ではなく行政刑罰である．主務大臣による行政処分（勧告，命令）がされた後，これに従わない（命令違反の）個人情報取扱事業者が最後に受ける制裁として，罰則が科せられるに過ぎない．

情報を「財物」と同様に取扱い，情報詐欺・情報窃盗等の直罰制を導入することの検討が，今後のわが国の刑事法制の抱える大きな課題の一つであろう．

4 技術的な状況と対策

本章では，フィッシング詐欺の技術的手口と，現在存在する代表的な対策技術について概観する．

4.1 技術的手口

被害者（A）に偽装サイトを信じ込ませるために，フィッシングにおいて利用される技術的手口には様々なもの

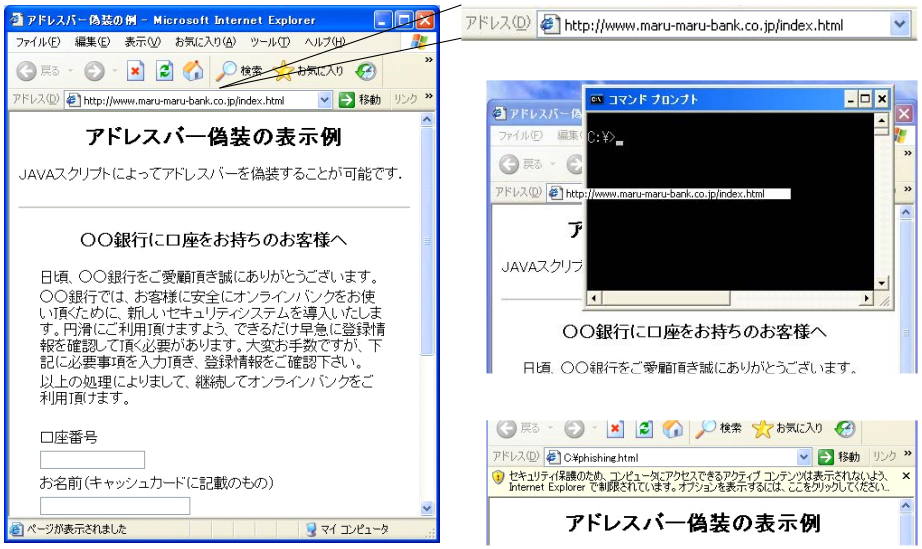

図 2: アドレスバー偽装手口例

がある．最も一般的な手口は④において，HTML メールでのリンクを実現する A タグの悪用である．HTML では，リンクを記述する際に，リンク先 URL とは異なった表示をすることが可能であるため，⑦において，例えば B とは明らかに異なる URL であるフィッシングサイトの URL を A に対して隠蔽することが可能となる．

また，②において，フィッシングサイトの見た目を偽装対象となる B のサイト（正当サイト）のそれに酷似させることも，⑧において A ををを騙すために有効である．ヨーロッパなどでは，フィッシングサイトを作成するための金融機関のロゴ画像などをパックした，フィッシングサイト作成ツールが数十ドルで出回っており，それらしいフィッシングサイトを簡単に作ることが可能である．

さらに，Web ブラウザ上のアドレスバーの表記を JavaScript によって詐称する手口も存在する．図 2 にこのアドレスバー偽装の例を示す．

左側のスクリーンショットでは，アドレスバーに maru-maru-bank の文字が表示されているが，(その拡大が図 2 右上)，これは JavaScript でのアドレスバー偽装によるもので，例えば，図 2 右中のように他のウィンドウを重ねることでポップアップの存在が明らかになる．このように非常に洗練された手口を使うフィッシングに対しては，コンピュータリテラシの高い利用者であっても，偽装を見破ることは困難であるといえる．なお，Service Pack 2 を適用した Windows XP では，このような JavaScript に対して，図 2 右下のような警告が表示される．しかし，この警告はフィッシング詐欺以外でも多くのサイトでも表示されるため，利用者が反射的に「OK」としてしまうことも考えられる．

4.2 技術的対策

このようなフィッシング詐欺に対して提案されている代表的な対策について説明する．なお，表 2 に示すように，法によって取り締まることができない⑥~⑧を中心に議論する．

4.2.1 サーバ証明方式

サーバ証明書を用いて，正当サイトであることを A に通知する対策である．例えば，⑧において A が情報を送信する際には，SSL のデジタル証明書を確認することで，情報送信先のサイトが正当サイトであることを検証することが可能となる．また，⑦において特定の正当サイトを利用する際に，A が専用のアプリケーションソフトを起動することでブラウザの動作を監視し，正当サイト以外のサイトを利用しようとした際に警告を発する対策も存在する．

ところが，フィッシングが問題化する以前からサーバ証明書は存在するにもかかわらず，フィッシング被害は増加の一途をたどっており，その効果は限定的であると考えられる．また，図 1 で示したように，フィッシング詐欺の特徴の一つは⑨以前には B の正当サイトを経由しないことにあるため，⑧を防ぐために B の正当サイトを経由することを前提にした対策では，フィッシングを防ぐことは困難と思われる．

これは，フィッシング詐欺の問題の別の側面も含んでいる．すなわち，図 1 に示すように，フィッシング

詐欺での情報の流れでは，正当サイトへのアクセスは⑨において初めて発生する．したがって⑧までの流れ（フィッシング）に関しては，B の正当サイト Web サーバのセキュリティ強度は影響を与えない．また，騙取された登録情報を用いた送金などの不正アクセスは，登録情報としては正規のもの（文字列など）を用いるため，B の正当サイト側でこれを見破るのは不可能に近い．故に，フィッシング詐欺において直接的には正当サイトの企業に “Web サーバ運営上の落ち度” は無いと考えられる．しかしながら，B の顧客 A との関係、預金者・消費者保護の観点ならびにフィッシング詐欺による風評被害などを考えると，落ち度がないにもかかわらず損害を被る可能性があると言え，これがフィッシング詐欺が企業に与える影響の大なるものであると考えられる．

4.2.2 ブラックリスト方式

⑦において，ブラウザで Web サイトにアクセスする際に，アクセス先サイトがフィッシングサイトかどうかを URL によって判断し，A に警告を通知する対策である．サーバ証明方式と比較して，A の確認操作や B の正当サイトを経由することを前提としないため，サーバ証明方式とは異なった効果が期待できる．

ただし，フィッシングサイトの寿命は 5.3 日程度であり，また 1 日平均 200 以上の新たなフィッシングサイトが報告される状況を鑑みると，ブラックリストの作成が困難であることが予想される．ブラックリスト方式は，リストに存在しない場合は “ 正当である ” と判断してしまうフェイルアウトな仕組みであるため，このように変動の激しいフィッシングサイトに逐次対応することには困難が伴うと考えられる．

4.2.3 その他の対策

⑤または⑥において，悪質なメールが A の目にふれる前に検知・排除することを狙ったスパムメールフィルタリング技術があり，これをフィッシングメールに適用している対策がある．フィッシングでは巨大ブランドを偽装した方が効率的なため，フィッシングメールはスパムメール的な大量送信となることが多いと考えられ，スパムメールフィルタの効果が期待される．但し，フィッシングメールの文面は正当なメールのそれに酷似しており，アダルトスパムメールのような不快な表現が含まれていないため，キーワードフィルタリングでは対策とはなり難い．

また，⑨において，騙取されたアカウント情報の再利用を排除するためにワンタイムパスワードなどが導入されている．マンインザミドル攻撃に対しては脆弱性が存在するが，一定の効果が見込める対策であると考えられる．

5 まとめ

本論文では，フィッシング詐欺について典型例を示し，法的・技術的観点からその現状を議論した．日本の現行刑法においては，有体物ではない “情報” を騙し取ることに対して詐欺罪は適用されないため，フィッシングによる情報騙取の被害者を救済することは困難である．したがって，実際の法適用においてフィッシング詐欺は，情報の騙取に成功した時点ではなく，その前後のプロセスにより摘発・起訴されている．情報を騙取する前の準備段階である著作権の侵害，不正アクセス，騙取後にその情報を利用して行う詐欺等，様々な犯罪類型の適用可能性を検討した．一方，技術的に洗練度を増すフィッシングに対して，代表的な対策である，サーバ証明方式およびブラックリスト方式について説明し，その効果と限界に言及した．今後は，フィッシングメールの文面やフィッシングサイトの構成など，情報を騙し取るため用いられるソーシャルエンジニアリング的な手口を考慮した技術的な防御対策が必要であろう。現行刑法が及ばない情報騙取に対する、技術の果す役割及び技術への期待は大きいと考える．

参考文献

[1] ケビン・ミトニック，ウイリアム・サイモン，“ 欺術（ぎじゅつ）－史上最強のハッカーが明かす禁断の技法 ”，ソフトバンク　ハブリッシング，2003.

[2] Anti–Phishing Working Group, Web Page, http://www.antiphishing.org/

[3] 警察庁，“平成 17 年上半期の不正アクセス行為の発生状況等について”，平成 17 年 8 月 18 日，http://www.npa.go.jp/cyber/statics/h17/image/pdf26.pdf.

[4] 藤木 英雄 他, “法律学小事典”, 有斐閣, 1988.

[5] 朝日新聞, 2005 年 7 月 5 日, 朝刊.

[6] 朝日新聞, 2006 年 2 月 7 日, 夕刊.

[7] 独立行政法人国民生活センター, “個人情報流出事故に関する事業者調査結果”, http://www.kokusen.go.jp/cgi-bin/byteserver.pl/pdf/n-20050325_1.pdf, 2005 年 3 月 25 日.