フィッシング対策協議会
Council of Anti-Phishing Japan

フィッシングレポート 2010

－　急増するフィッシング詐欺の実態　－

平成 22 年 11 月

フィッシング対策協議会

技術・制度検討ワーキンググループ

目次

1. フィッシングの動向

1.1. 国内の状況

2009 年の後半から、国内におけるフィッシングの報告件数が急増している（図 1-1）。

フィッシング対策協議会に対するフィッシング情報の報告件数は 2010 年 2 月までで、既に対前年度で 87%増（2008 年度 151 件から、2009 年度 283 件）となっている。また、フィッシングサイトのユニーク URL 件数は、前年度の 3.8 倍（2008 年度 68 件から、2009 年度 260 件）となり、報告件数以上の増加となっている。これは、フィッシングサイトのテイクダウンを回避するなど、フィッシング手法の高度化や、関与する犯罪者の増加を反映しているものと考えられる。

一方で、フィッシングよりブランド名を悪用された企業の件数は、横ばいないし減少（2008 年度 57 件から、2009 年度 46 件）しており、引き続き、有名なサイト、つまり犯罪者から見た場合に効率的なサイトを対象とした攻撃に集中していることがわかる。

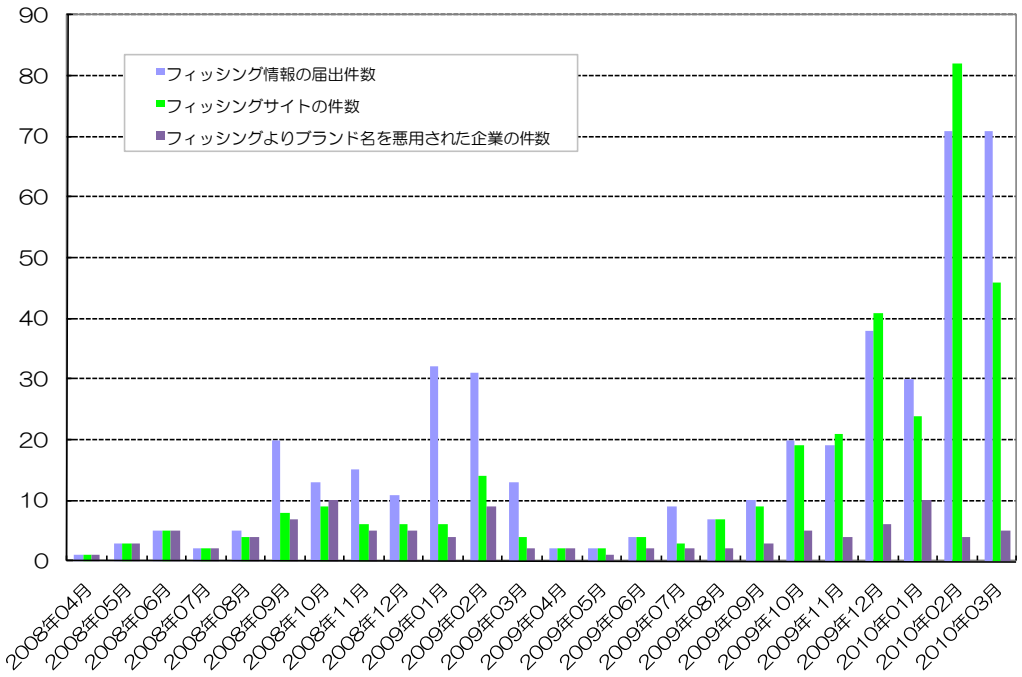


図 1-1　フィッシング対策協議会への報告件数等

また、国家公安委員会・総務省・経済産業省の発表によれば、警察庁に報告のあった不正アクセス行為として、識別符号窃用型不正アクセス行為（ID 窃盗による不正アクセス行為）が急速に増加している（図 1-2）。また、その手口を見ると、平成 20 年は利用者のパスワードの甘さをついたものが大多数で、フィッシングによるものはわずか 5%に過ぎなかったものが、平成 21 年にはフィッシングが大半（83%）となっている（図 1-3）。

図 1-2　識別符号窃用（ID窃盗）型不正アクセス行為の検挙件数[1]

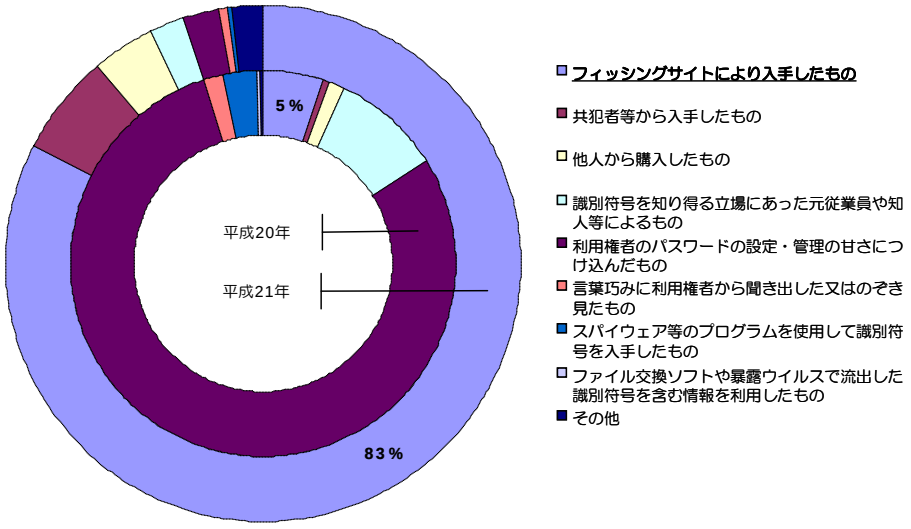


図 1-3　不正アクセス行為に係る犯行の手口の内訳[2]

従来、国内はフィッシング被害について、諸外国よりも影響が少ないと言われてきたが、2009 年末から状況は急速に変化しつつある。事業者はもとより、一般消費者においても、フィッシングの脅威に対する正しい知識を普及させる

[1] 国家公安委員会・総務省・経済産業省,「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」,http://www.npa.go.jp/cyber/statics/h21/pdf53.pdf、より株式会社三菱総合研究所が作成

[2] 同上

ことが、被害の拡大の防止には欠かすことができない。

■近年の不正サイトの状況　ーaguse[3]の調査結果からー

aguseによる調査[4]による危険度の高いサイトの検索結果によれば、一般に、脆弱性に関するレポートでは、日本は比較的安全で米国や中国に危険度が高いとされているが、必ずしも日本に設置されたサーバが安心とは言えないことがわかった。この結果は調査対象が、危険性のあるサーバの全てではなく、日本国内のエンドユーザの目にとまり、実際にリーチできるurlが対象となったためと考えられる。

また迷惑メール送信元や迷惑メールに紐付くマルウェア配布元となるドメインは、一般に取得から経過年月が浅いことが多いが、信頼・実績のあるドメインであっても Gumblar などによる Web 改ざんされる事例があり、安心できない状況となっている。

ブログや SNS などを利用することにより簡単に情報配信ができるようになった結果，2～3 年経過して管理されない HP が存在している。このようなところにコメントやリンクを残し，脅威の潜むサイトに誘導するケースも見受けられる。

具体的な例を一つ示すと、あるゲーム関連ドメインにはマルウェアが仕込まれているが、当該ドメイン管理者は他のドメインも同一サーバ上に横展開している。

これらは国内の一般ユーザが製作したコンテンツを frame でマルウェア配布サイトと抱き合わせた構成になっている。

抱き合わせされた被リンクサイトは、しばらく更新されず管理が不十分となっていることが多い。一見したところ問題ないように見えるのが、フィッシングサイトと同様な危険性を含んでいる。

従来はアダルト、出会い系、精力増強剤に関するサイトが調査されることが多かったが、最近ではカテゴリーに関係なく、季節に応じた旬なテーマのサイトが調査される傾向にある。例えば不景気になると司法書士、便利屋、情報商材等のサイトであるとか、オリンピックの際は画像、動画コンテンツを抱えるサイトといった傾向である。

表面上は問題ないように見えるサイトであっても、その背景情報により正規サイトであることを確認することが重要であると思われる。

[本稿執筆担当：白石 知宏（アグスネット株式会社）]

---

[3] aguse（http://www.aguse.jp/）ではユーザが安心してインターネットを利用できる環境を整えるために，サイトに関する背景情報を事前に調査できるサービスを提供している。

[4] 調査の概要

対象：　http://www.aguse.jp/ のウェブ調査に入力された URL
期間：　2010/01/01 から 2010/01/31 の１ヶ月間
ユニークユーザ数：約 10 万人/月

※：aguse に入力された URL は、必ずしも不正なサイトだけではなく、当該サイトの安全性を確認するために入力されたものを含む、安全性に対してユーザの懸念が高いサイトが検索上位に来る。

1.2. 海外の状況

米国で設立されたフィッシング対策問題に関する国際組織 APWG（Anti-Phishing Working Group）の調査によれば、2009 年のフィッシング情報の報告件数は前年比約 23%増、同フィッシングサイトの件数は約 80%増であるなど、引き続き脅威が高まりつつける状況にある。

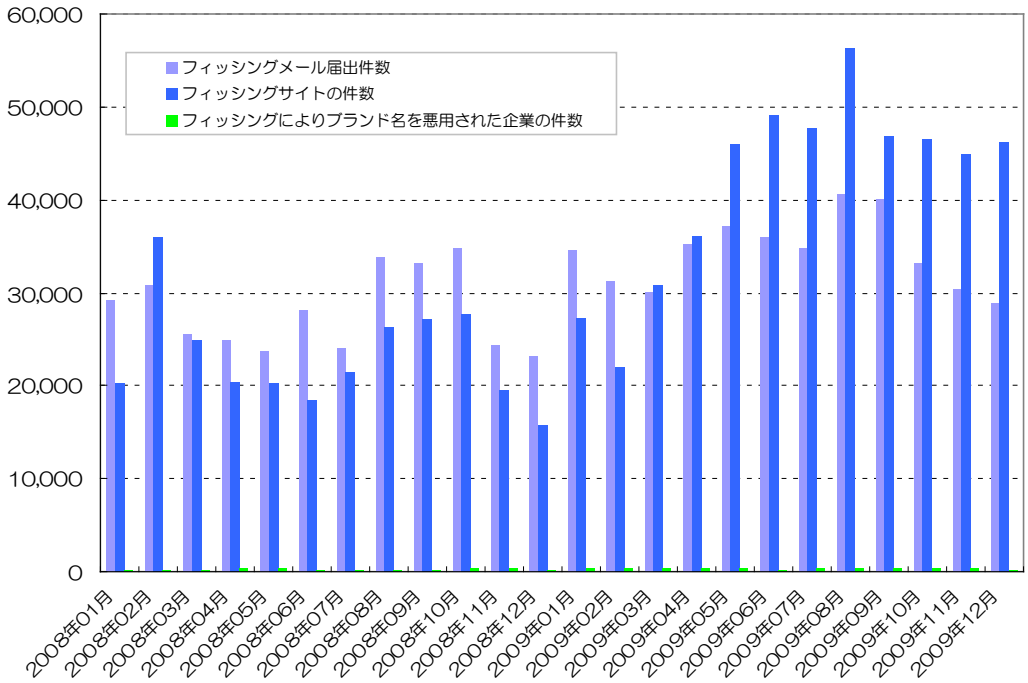


図 1-4　APWGへの報告件数等[5]

しかしながら、絶対数こそ少ないものの、国内におけるフィッシング被害は、世界のトレンドを上回る伸び率で増加していることがわかる。例えば、フィッシング情報の報告件数でみれば、世界全体の 23%増に対して、日本では 40%増などとなっている。

[5] APWG (Anti-Phishing Working Group), "Phishing Activity Trends Report"、http://www.antiphishing.org/index.html、より株式会社三菱総合研究所が作成

2. 新たな脅威の動向

フィッシングとは、ID 窃盗を行うための手法の一つであるといえる。フィッシング対策協議会では、従来型のフィッシングに留まらず、事業者からの ID 窃盗につながる脅威についても監視を行っている。

フィッシング対策協議会においても、最近 ID 窃盗がオンラインバンクやクレジットカード情報だけでなく、ゲームアカウントやソーシャルメディア、FTP のアカウントなど広く広がっているのを確認している。Internet によるサービスの拡大により、一般消費者はより多くのオンラインアカウントを持つ傾向にあり、オンラインアカウントの重要性も増しつつある。
それによりオンラインアカウントを含む ID 窃盗もより広範に、より巧妙になってきている。

従来のようにオンライン銀行やクレジットカード以外にも様々な目的で、下記のような情報が狙われている。よって、ユーザは、自身ではそれほど価値がないと思うようなアカウントにも十分安全に気を配る必要がある。

- クレジットカード情報：オンラインでの不正な買い物をするために狙われる。
- オンラインゲームアカウント：仮想世界であるオンラインゲーム内でのアイテムが価値を持ち、それが現実世界で売買が行われることにより、そのアイテムなどを取得するためにオンラインゲームのIDが狙われる。
- オンラインオークションアカウント：身元を隠し、不正出品などのオークション詐欺を働くために、すでに利用されているオークションになり済ます目的で、アカウントが狙われる。
- ソーシャルメディアのアカウント：ソーシャルメディア内では、ユーザはそこに書かれた情報をより信頼する傾向にある。その点を利用して、ほかの詐欺に誘導するためのアカウントのなり済ましのために、既存のアカウントが狙われる。あるいは、ユーザはIDとパスワードを複数のサービスで同じに設定している傾向があり、メールなどのより重要なサービスを悪用するために狙われる。
- BlogやWebサイトなどその他のオンラインサービスアカウント：そのユーザのBlogやWebサイトを改ざんし、罠を仕込む、あるいはそのサイトに侵入し、より価値の高い情報を取得するのに利用するために狙われる。

また、ID 窃盗に使われる方法もカードのスキミングのような直接的な方法から、古くから使われる電話によるソーシャルエンジニアリングなどもあるが、現在はフィッシングを始めとした Internet を介しての ID の取得が多くなっている。ID 窃盗関連の技術として下記のような技術が利用される。

・ カードのスキャンニング、スキミング
・ ソーシャルエンジニアリング（なりすまし）
・ フィッシング
・ ファーミング
・ トロイの木馬
・ ドライブバイダウンロード
・ サイトへの侵入

本ステータスレポートでは、ターゲットのアカウントの中で、オンラインゲームのアカウントと ID 窃盗の手法として最近増えているドライブバイダウンロードを取り上げて解説する。

2.1. オンラインゲームにおけるID窃盗の状況

(1) 概要

オンラインゲームは幅広い層に根強い人気があり、毎年多くのタイトルが発表されている。オンラインゲームの収益形態は、課金されない完全にフリーなものもあるが、多くの場合、「アカウント課金」と「アイテム課金」の二つに大別できる。近年の傾向として、後者を採用するケースが非常に多い。前者の場合、ゲーム開始時にアカウントを作成し、それを維持するために月額料金などを決済することになるが、ゲームユーザにとっては「最初はお金がかかる」ことは敷居が高いため、最初はお金がかからず、まずは多くのユーザを集め、ゲームが進行するにつれてゲームキャラクターに特別なアイテムや衣装などを付与できることに対して課金するという形態が主流になってきている。これにより、オンラインゲーム事業者からみると一顧客当たりの収益単価が増え、ゲームユーザから見ると、複数のアカウントを一人で取得し、同一ゲーム内でも様々なバリエーションで楽しめるという実態がある。
このように、オンラインゲームを楽しむためには、ユーザはまずアカウント ID とパスワードのセットを作成することになるのだが、これらを窃盗するマルウェアの出現が後を絶たない現状がある。
窃盗された ID・パスワードは、それそのものが売買されるケースもあるが、

多くの場合、悪意ある者は窃盗された ID・パスワードを使用してゲームにログインし、そのキャラクターが所持しているアイテム類を悪意ある者が所有するキャラクターに渡す。それらアイテム類をゲーム内で売り捌いて「ゲーム内通貨」を得る。一方で、ゲーム内通貨を現実世界の通貨に換金する業者（RMT（Real Money Trade）業者）も存在し、ここでゲーム内の世界と現実世界が繋がっているといえる。

(2) 被害の状況

オンラインゲームのID情報をゲームユーザから窃盗する手法は、以前はインターネットカフェのPC端末にID・パスワードを窃取するマルウェアが仕掛けられる例が多く確認されていた。近年、オンラインゲームユーザのPC端末が、トロイの木馬として動作するマルウェアに感染する例が増加しているほか、ゲームサイトを装ったフィッシングサイトも数多く発見されている（図2-1）。これらのマルウェアは、ゲームの攻略サイト（もしくはそれを装ったサイト）に仕掛けられていたり、USBメモリ感染型のマルウェアドロッパ[6]によりダウンロードされたりすることが多い。ウイルス対策ソフトが導入され、定義データベースが最新に保たれているPC端末においては、これらのマルウェア侵入時点でそれを検知できる可能性が高いが、ウイルス対策ソフトを動作させているとPC端末の動作が重く感じられたりオンラインゲーム自体に備えられている機能とウイルス対策ソフトの相性が良くない場合がある[7]ことから、オンラインゲームユーザの中には、ゲーム進行を優先するがあまり、ゲームプレイ中はウイルス対策ソフトをオフにしたり、ウイルス対策ソフトを導入しない人もいる。当然ながら、こういった状態のPC端末には、マルウェアによって容易に侵入されてしまう可能性がある。

オンラインゲームの ID を狙うマルウェア数は、あるベンダのシグネチャ数を例にとると、全シグネチャ数の 5%を超えており、亜種が非常に多く出回っていることが分かる。また、亜種を簡単に作成するためのツールもブラックマーケット上には流通しており、日々新たな亜種が作成され続けているのが現実である。

マルウェア以外では、オンラインゲーム事業者に勤務していた者が、退職後にオンラインゲーム事業者の管理サーバに不正侵入したり、ユーザ情報を持ち出して不正行為をはたらくなどの例があり、人為的・管理上の課題もある。

---

[6] マルウェア等をダウンロードするプログラム

[7] マルウェア対策製品の中には「ゲームモード」と呼ばれる機能を有し、ある程度オンラインゲームユーザの利便性を考慮したものもある。

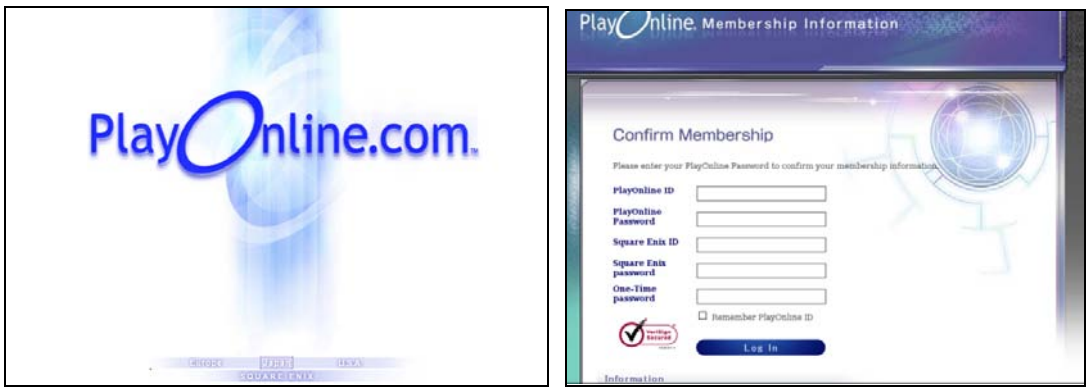


図 2-1　オンラインゲームのフィッシングサイトの例

(3)　対策と課題

　オンラインゲームの ID はマルウェア経由の窃取が多いことから、ユーザの PC 端末においては、一般的なマルウェア対策（ウイルス対策ソフトを導入し、定義データベースを最新にすること）が有効な対策の一つであると言える。また、ゲームサイトを騙るフィッシングサイトについては、アクセス時にドメイン名を確認するなどの注意も必要である。
ただ一方で、先述の RMT 業者の存在が示すように、業界構造的な課題があることも考慮する必要がある。ゲームタイトルの中には、ゲーム内でユーザ同士が授受できるアイテム（特にゲーム内通貨で高価取引されるものなど）を制限したり、不正な行為をはたらくユーザアカウントを停止したりする措置を積極に行っているものもあるが、これらの対策は当然のことながらあくまでもオンラインゲーム事業者の裁量に一任されている。また事業者側は、不正行為対策よりもヒットするゲームタイトルの開発とそのプロモーションが主たる事業活動であるため、これらの対策を率先して打っている状態であるとは必ずしも言えない。
更に、不正に入手した ID でオンラインゲームに参加することは検挙例もあり犯罪であるという認識が広がりつつあるが、ゲーム内での個々の所作（アイテムの交換や取引）は現実世界のものではないため強権機関による取締は依然として困難である。不正使用した ID で得たゲーム内通貨を現金化した、という流れが証明できれば、これは犯罪行為と見なされ検挙例もある。ただし、ゲーム内通貨を現金化する行為自体は日本国内では取締法が無く、事業者の倫理に委ねられているのが現状である。

[本稿執筆担当：前田 典彦（株式会社 Kaspersky Labs Japan）]

2.2. Gumblar攻撃に利用されたドライブバイダウンロード

(1) 概要

ドライブバイダウンロードはユーザがブラウザを使って、Web サイトを訪れたときに、マルウェアをインストールさせる方法で、古くは 2003 年頃から Adware や Spyware のインストールの手法として使われだした。最近は Gumblar に代表されるように、マルウェアの感染手法として主流になりつつある。当初は IE の ActiveX の脆弱性を使い、音楽の歌詞のサイトや Internet ラジオのサイトなどを訪問したユーザの PC に広告プログラムを勝手にインストールさせる手段として使われた。

手法としては下記の図のように Web ページの中に Hidden 属性の IFRAME などを埋め込み、IFRAME で読み込まれるページにソフトウェアの脆弱性を利用するマルウェアを置く。ユーザは正規サイトにアクセスしているつもりでマルウェアを読み込んでしまう。

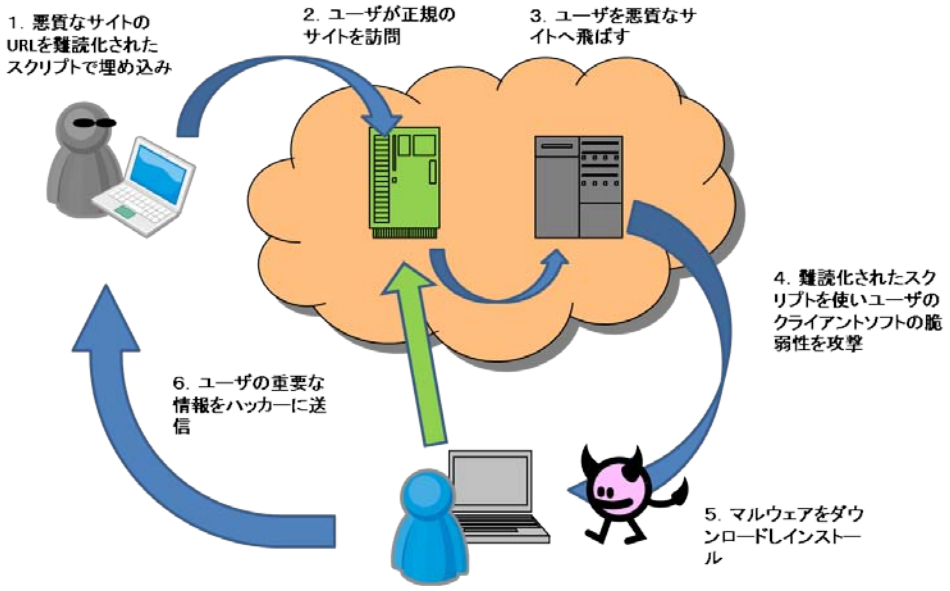


図 2-2 ドライブバイダウンロードの方法

一部の過激な Adware はそれをなるべく多くの PC にインストールさせるために、インストールに対してアフィリエイトのお金を支払うペイパーインストール(PPI)というマーケティング手法を行った。このため、このアフィリエイトのお金を稼ぎ出すために、ドライブバイダウンロードのような悪質な方法を使ってインストールさせる手法が広まった。

現在、Adware については米国の FTC(連邦取引委員会)の取り締まりにより、その組織がなくなったが、現在、同じ PPI の手法を使って、偽のセキュリティソフトが同様のマーケティング手法を行っている。

よって、ドライブバイダウンロードを行う組織とその結果インストールされるソフトウェアを作成する組織は別で、分業されていることが多い。

(2) 攻撃の手法

ドライブバイダウンロードはそのサイトをユーザがブラウザで読み込む必要がある。ドライブバイダウンロードを仕掛けるサイトにおびき寄せる行為として以下のような手法が使われる。

- リンクを含んだメール・IM などによる方法
- オンライン広告への悪質なスクリプトの挿入
- SEO を使った検索結果の汚染
- 掲示板や Wiki、ブログのコメントなどへの書き込み
- ソーシャルネットワーク内の仲間へのメッセージとしての書き込み
- ホストティング事業者のルータの脆弱性を使い、ARP spoofing を利用しての転送
- Web の改ざんにより、リンクの埋め込み
  サイトの脆弱性を狙った直接の改ざん
  サイト管理者の PC に感染して、その PC 内の HTML の改ざん
  サイト管理者のコンテンツ更新のためのアカウントを窃盗したうえでの改ざん

最後の Web の改ざんについては、以前はサイトのサーバ側に含まれる脆弱性を利用して行われていたが、昨年から問題になっているのが、サイト管理者のクライアントのコンテンツ更新のためのアカウント ID を窃盗し、直接サイトのコンテンツを書き換える改ざんである。そのアカウント ID の窃盗にも、ドライブバイダウンロードが使われるなど、ドライブバイダウンロードは現在の攻撃の手法として、主流となってきている。

サイト管理者の PC に感染し、PC 内のコンテンツを直接書き換える方法が 2005 年頃から行われていたが、最近はコンテンツをアップロードするのに利用する FTP アカウントを盗み出し、外部からサーバのコンテンツを直接書き換える方法が、広く使われている。

また、特にFTPのアカウントを狙ったトロイの木馬としてはPWS-Per-FTP[8]や

[8] http://vil.nai.com/vil/content/v_144460.htm

TrojanDownloader:Win32/Palev.A!dll [9] などが報告されており、Win32/Palev-AはプロセスにInjectionされ、FTPサーバとの通信されるIDとパスワードを盗む。
実際、いつくかのドライブバイダウンロード作成用のツールはサーバの FTP アカウントを使ってサイトの改ざんを行う。よって、Web サーバ側の脆弱性をチェックしているからといって安心できない。このように Web の改ざんによる方法が増えてきているのと、ユーザが多く訪れる大手のサイトが狙われているのが最近の傾向である。

また、ドライブバイダウンロードのサイトも以前は特定の脆弱性のみを狙った簡単なものであったが、現在は複数の脆弱性を狙った巧みなスクリプトになっている。そのようなサイトを作るためのツールが 2006 年頃に Mpack や Icepack の名前で登場し、現在も “Yes Exploit System”や” Eleonore Exploit Pack”など多くの脆弱性を突くスクリプトを自動生成できる攻撃ツールが作成され、オンラインで販売されている。図 2-3 の"Yes Expolit Pack"の販売ページのように、ドライブバイダウンロードは商用ベースとしていろいろなツールが開発され、難しい知識がなくとも簡単にドライブバイダウンロードのサイトを作成することができる。

[9]http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=TrojanDownloader%3AWin32%2FPalev.A!dll&ThreatID=-2147348143

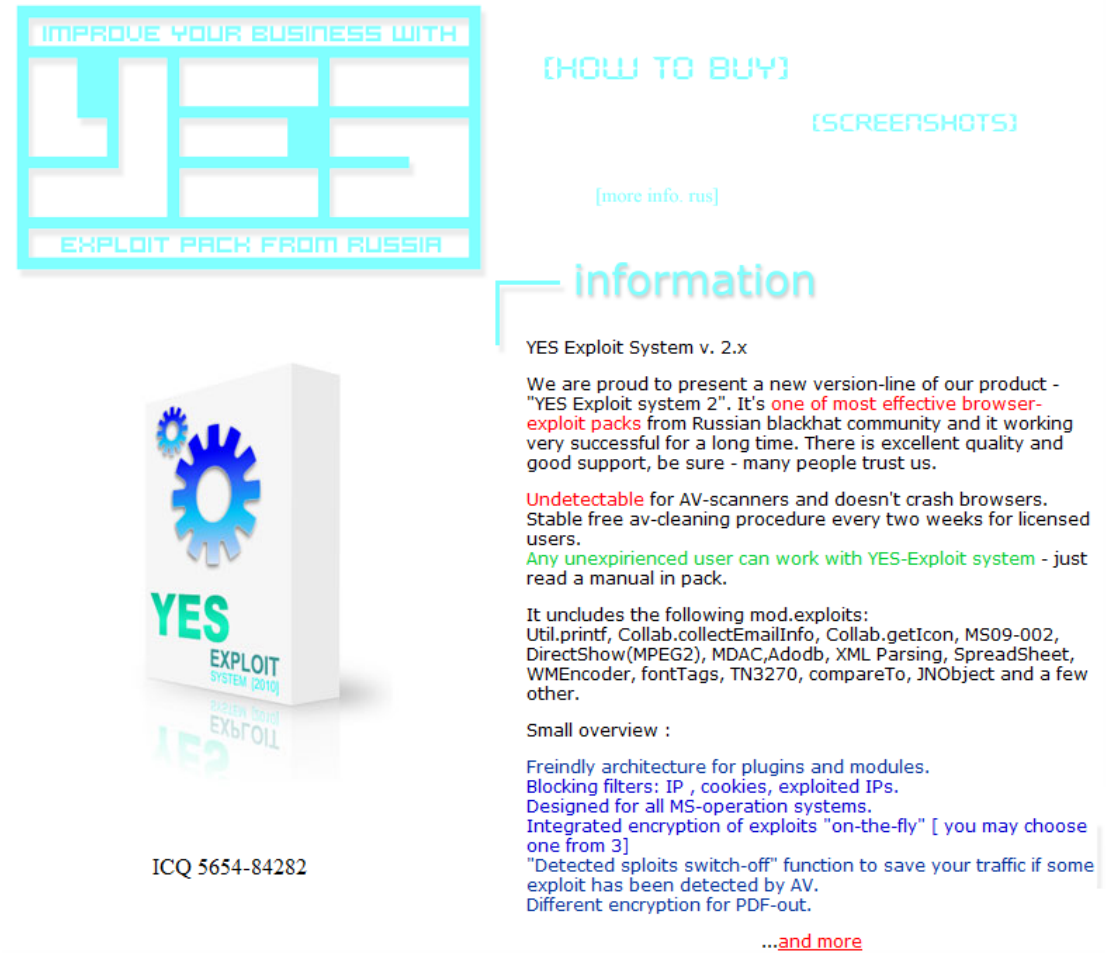


図 2-3 Yes Exploit System の販売ページ

(3) 対策

ドライブバイダウンロードは下記のようなセキュリティ対策技術によって防御可能である。

・ 悪質のあるスクリプトの検知による防御

スクリプトによるドライブバイダウンロードの実行を行うスクリプトを検知し、その実行をブロックする。

ほとんどのセキュリティ対策製品でサポートされており、最初の入り口で防御できるため、効果的ではあるが、基本的にスクリプトは簡単に改編可能であるため、多くのバリエーションを作成することができ、スクリプトの検知は非常に難しい。AV ベンダはヒューリスティック技術での検知を提供しているが、誤検知を防ぐ事が難しい。

たとえば、多くの悪質なスクリプトは難読化されているが、難読化は正規のサイトでメールアドレスをスパマーに刈り取られないようにするために使っていることがあり、必ずしも難読化されたスクリプトを含んだページが罠サイトとは限らない。

・ ホスト侵入防御システム(HIPS)を使った脆弱性の検知・ブロック

マルウェアのインストール・実行を行うために利用されるブラウザまたはブラウザから自動実行されるアプリケーションの脆弱性の攻撃を検知して、その攻撃を防御する。

実際の攻撃か行われる前に検知・ブロックは可能であるが、基本的に既知の脆弱性にしか対応できないため、ゼロディ攻撃へは対応できない。また、HIPS をサポートするセキュリティ製品が限られていることと、誤検知の可能性がある。

・ ウイルス対策技術によるダウンロードされるマルウェアの検知・ブロック

マルウェアが PC にダウンロードされるときに、検知して防御する。

アンチウイルス製品すべての製品でサポートされているが、最近はシグネチャの作成がマルウェアの出現に対応できていない。そのため、ジェネリックやヒューリスティックの検知の強化を行っているが、それは逆に誤検知を生むこととなっている。

・ スクリプトやマルウェアのホスティングサイトの識別とブロック

ユーザが悪質なサイトを訪問しようとしたときに IP アドレスやドメイン名を基準に判断して、そのサイトへの訪問を止める。

すべての悪質なサイトの情報の収集を完全に行うことが難しいことと、ホスト名もランダムに頻繁に変更され、Fast Flax のようにボットに感染した PC を使い、DNS のホスト名の接続先をランダムに変更するような方法が使われた場合の対応は難しい。

・ インストール・レジストリ改ざんの検知・ブロック

マルウェアの実際のインストールはシステム領域に行われることが多く、また、自動実行のため、レジストリの改ざんが行われる。このシステム領域への書き込みとレジストリの変更を検知して、実行を阻止する。

実際の実行を防ぐことができるので、ID を盗まれるなどの実際の被害を防御することができる。また、シグネチャ等に依存しないため、未知の攻撃やマルウェアによるものでも防御できる。この方法にはセキュリティソフトの

監視による方法と Windows Vista 以降でサポートされた UAC による方法がある。セキュリティソフトの監視による方法は、基本的に HIPS と同じ技術でサポートされるセキュリティ対策製品は限定される。もともと、Windows NT には権限の機能が存在するため、利用するユーザの権限を制限すれば、システム領域へのファイルのインストールやレジストリの改ざんは防ぐことが可能である。ただし、多くのユーザは制限アカウントではソフトのインストール等ができないため、管理者グループのアカウントで利用している。そのため、Vista では、管理者権限のアカウントであって、管理者権限が必要な実行をする場合は、昇格プロンプトを出す UAC を導入した。これを利用すれば、権利者権限のアカウントで利用していても、勝手なシステム領域へは書き込みやレジストリの改ざんを防ぐことができる。

上記にようにドライブバイダウンロードを防ぐために、いろいろな技術的な対策が存在する。特に最後に紹介した対策である Vista 以降でサポートされた UAC はドライブバイダウンロードを含むすべてのマルウェアのインストールを防御する上で効果的な機能ではあるが、最終的に、ユーザが騙されて許可をした場合には防ぐことはできない。よって、技術と共にユーザの教育を行うことが重要である。

3. 総合的対策の確立に向けた課題

3.1. 技術的課題

(1) フィッシング対策の現状と課題について

当協議会に報告されるフィッシングサイトの件数は 2009 年 5 月以降増加傾向にある。これらの急増するリスク低減策には様々なアプローチがある。ここではそれぞれの課題に対して、フィッシング対策協議会が行った幾つかの技術的なアプローチを紹介する。

・ フィッシングサイトのテイクダウン

消費者などから報告されたフィッシングサイト URL を ISP やセキュリティ組織などに連絡し、フィッシングサイトの停止依頼を行い、実際にフィッシングサイトを停止することをフィッシングサイトテイクダウンと呼ぶ。テイクダウンに必要な時間は事例によりまちまちであり、海外にフィッシングサイトを立ち上げられている場合や、Fast-Flux といった手法を用いてサイトを立ち上げられている場合は、テイクダウンまで数週間を要することがある。テイクダウンについては ISP やセキュリティ組織との信頼に基づく協力関係を持つことが大切であり、フィッシング対策協議会ではテイクダウンの業務を長きにわたって実施している JPCERT/CC にこの作業を依頼している。協議会では 2009 年 4 月より 2010 年 3 月 1 日までの間 214 件の報告を受けており、JPCERT/CC と協力の上、多くのフィッシングサイトをテイクダウンしている。

・ フィッシングフィルタリング機能 (ツールバー、ウイルス対策ソフトなど)

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 URL の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を主要ブラウザ、各ウイルス対策ベンダ、インターネットサービス事業者などが提供している。

このフィッシング検出機能は、フィッシングサイトが停止するまでの期間のユーザ保護として有効だと考えられる。ユーザが被害に遭うリスクを低減させることを目的として、当協議会でも 2010 年 2 月 1 日よりヤフー株式会社の「Yahoo!ツールバー」、Kaspersky Labs Japanなどにフィッシングサ

イトURLを提供している[10]。

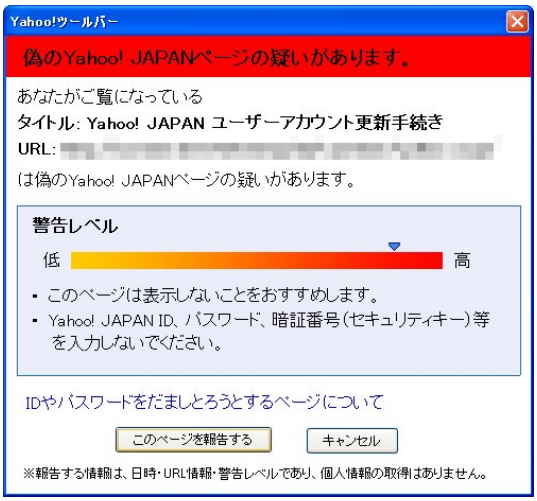


図 3-1　フィッシングフィルタリング機能 (Yahoo!ツールバーの場合)[11]

・ フクロウ先生のフィッシング警告ページ

フクロウ先生のフィッシング警告ページは APWG と米国カーネギーメロン大学が共同で開発したフィッシング対策教育用 Web ページである。

コンテンツを削除したフィッシングサイトの跡ページにはページが見つからないなどのエラーメッセージが表示される。このプログラムは閉鎖したフィッシングサイトの跡ページに警告ページ「フクロウ先生のフィッシング警告ページ」を表示させることで、フィッシングサイトであったことをユーザに認識させ、手口の紹介やフィッシングサイトに関する注意事項などを学ばせることを目的としている。実際には、フィッシングサイトの跡ページにリダイレクトの設定を行い、APWG 内のページに転送して表示させる。

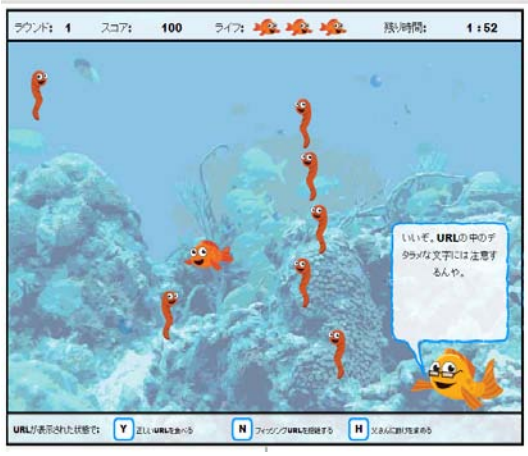
2010 年 3 月現在、フクロウ先生のフィッシング警告ページは日本語を含む 17 の言語に翻訳され、全世界に展開されている。

[10] http://www.antiphishing.jp/
[11] http://toolbar.yahoo.co.jp/

図 3-2　フクロウ先生のフィッシング警告ページ[12]

・ フィッシングフィル(教育コンテンツ)

Wombat Security Technologies 社が開発したフィッシング用教育ゲームである。フィルという魚のキャラクターを動作して、エサをモチーフとした Web サイトの URL をもとにフィッシングサイトの正/偽の判定を行う。ゲーム開始時にはフィッシングサイトの見抜き方の解説ページがあり、終了時にはラウンド毎の解説ページがある。これらを通してフィッシングを認知していない消費者がゲームを楽しみながらフィッシングサイトの見分け方を体得することを目的としている。当協議会ではこのゲームを日本の消費者向けにローカライズし公開した。



[12] http://education.apwg.org/r/jp/index.htm

図 3-3　フィッシングフィル[13]

フィッシング対策においては日々変わる攻撃手法に応じた、タイムリーな対策が求められている。本項で紹介した対策もほとんどが本年度開始された取り組みである。

(2)　技術的な被害防止の取り組み

様々なセキュリティベンダや関係者が以下のような技術の普及を通じてフィッシング被害低減への努力を進めている。

・ EV SSL証明書

フィッシング詐欺の防止などを目的として、世界の認証局及びブラウザベンダによって CA/Browser Forum が設立され、その中で標準化された認証プロセスのもと発行された証明書が EV SSL 証明書である。EV SSL 証明書は法人登記されている民間企業及び政府機関にしか発行されない。そのため、Web サイトの信頼性の面でフィッシング詐欺の防止に効果を発揮するといえる。また、発行の際、申請責任者の権限や事業を行っている住所の確認など厳密な審査が行なわれる。この EV SSL 証明書を利用しているサイトにアクセスした場合、アドレスバーが緑色に表示され、会社名及び認証局の情報が表示される。

・ 多要素認証

多要素認証とは、通常使用される、ID とパスワードの組み合わせだけでなく、複数の情報を認証に利用する認証方式を多要素認証と言う。多要素認証が利用されている例としては暗証番号（4 桁の数字）と生体認証（掌紋のパターン）の両方を用いている銀行の ATM などがあげられる。またハードウエアトークンと事前に決めたパスワード（PIN などとよばれる）を利用するワンタイムパスワード認証もその一例である。

ハードウエアトークンには一定間ごとに変化する、ワンタイムパスワード(ランダムな文字列など)が表記される。このワンタイムパスワードを利用した場合、通信経路上でパスワード情報を盗まれたとしても、不正アクセスはできない。また、仮にハードウエアトークンが盗難に遭っても、トークンに表示されるパスワード以外に PIN が必要となる為、危険性は低い。

[13] http://www.antiphishing.jp/phil/

・ 送信ドメイン認証

送信ドメイン認証とは、メール送信者情報のドメインが正しいものか判断することができる仕組みである。メール送信時、送信者情報を詐称することが可能な為、フィッシングメールや迷惑メールの多くのは、送信者情報を詐称して送信される実態がある。送信ドメイン認証が多く普及することで、送信者情報のドメインを詐称しているメールの判定が可能となり、正規の送信者を騙って不正サイトへ誘導するメールなどを、フィルタリングすることが可能となる。

ここで紹介した技術は、主に金融機関で積極的な採用が始まっており、今後、SNS やオンラインゲームなどのコミュニティサイトなどでも、採用されていくと思われる。このような技術を効果的に組み合わせることで、フィッシング被害を抑える事が可能となる。

(3) 新たな技術に対する課題

今後、フィッシングに関して、新たな技術的対応が必要となるであろう課題は以下のように考えられる。

・ 日本などのマルチバイトTLD

フィッシングサイトと正規サイトを見分ける上では URL が大切なポイントである。近年ドメイン名の多言語化が進んでいる。これらはドメイン名の表現力を高め、特に英語やアルファベットに不慣れなユーザにとってインターネットを使いやすくすると言う効果がある。一方で表現力が高まることは、ドメイン名の偽装の危険性を高める。また現在日本においては多国文字国別ドメイン（IDN ccTLD)、つまり「.日本」の導入が検討されている。新規 TLD の追加にあたっては、例えば"antiphishing.日本"のドメイン名が"antiphishing.jp"の保持者に優先的に割り当てられるような配慮がされることが重要である。

・ 携帯サイト向けのフィッシングの増加

諸外国と比較して日本のユーザは携帯電話を通じて、メールや Web を利用することが多いとされている。一般に携帯電話は画面のスペースなどの物理的制約からアドレスバーなどの PC では必ず表示される情報が省かれてしまう。これはアドレスバーを通してフィッシングサイトを見分ける対策を進める上での課題である。

実際に 2009 年 12 月にフィッシング対策協議会に対して、いくつかの携帯電話から閲覧されることを前提としていたとおもわれるフィッシングサイトが報告された。今後同様の手口が広まる可能性があり、携帯電話でも容易に URL を確認するための機能を加えることはフィッシング以外の不審サイトの対策としても重要なポイントと思われる。

・ 短縮URL問題

現在、急速に利用が広まっている Twitter などのマイクロブロギングサイトでは 1 投稿の文字数が極めて厳しく制限されている。このようなサイトでは長い URL 短縮するサービスなどが一般的に利用されている。たとえば bit.ly というサービスを利用すると、

"http://www.antiphishing.jp/information/information821.html"

という長い URL を*"http://bit.ly/cqcluo"*と短縮することが可能である。これらのサービスは今後も利用が広まることが予想されるが、実際にアクセスするまで自分が開こうとする URL が一切確認出来ないという問題がある。一般ユーザが Web をブラウズする際に URL に注意を払うことを引き続き啓発することが、これまで以上にもとめられるだろう。

このような問題に対して、どのような取り組みが可能なのか、協議会では引き続き検討を行っていきたい。

3.2. 制度的課題

近時は、サイバー犯罪の件数が年々増加の傾向にあり、その手法・技術も高度化している。当協議会としても、フィッシング行為等に対する注意喚起・啓発に努めているところであるが、フィッシングの被害に遭うケースは後を絶たない。

サイバー犯罪については組織化・分業化している傾向が指摘されているところであり、フィッシングも例外ではない。当協議会の検討でもフィッシングにおける組織化・分業化の傾向が強まっていることが確認された。会員企業からは、他人のメールアドレスとパスワードを盗み取るプログラムを作成して第三者に売買した事例、作成したプログラムによってメールアドレスとパスワードを盗んで第三者に売買した事例、他人から ID を購入して第三者に転売した事例等について報告があった。いずれの事例においても、他人の ID やメールアドレスは第三者によって財産的犯罪に悪用されていた。

日本では、フィッシングサイトを開設するなどによって他人の ID やメールア

ドレスとそれらのパスワード（以下、「ID 等」という。）を取得する行為及び不正に取得された ID 等を第三者に提供する行為を処罰する法律がないため、そのような行為を行う者が野放しにされている。他人の ID 等を悪用した財産的犯罪が摘発された場合であっても、他人の ID 等の取得・第三者への提供等に関与したにとどまる者はいわゆる不正アクセス禁止法に抵触しない限り不可罰とされる。

いまや、インターネットは国民の日常生活において欠くことのできないインフラとなっており、ID 等はインターネットにおける認証等で重要な社会的機能を行使している。しかし、現在の法制度は、ID 等の取得や悪用を伴う組織化・分業化された行為に対して十分に対応できる内容とはなっていないため、ID 等をターゲットにした組織的かつ大規模な犯罪的行為を誘発する恐れがある。そのようなときには、国民の安全なインターネット利用を阻害し、電子決済システムが混乱し、国民経済にダメージが生じることが懸念される。また、その被害は、今後はよりいっそう深刻なものになると思われる。

当協議会としては、引続き、他人のID等を不正に入手しようとする行為を技術的に防止する手段について検討していくが、技術的方法によってすべての問題を解決できるとは考えない。他人のID等を不正に取得しようとする行為、不正に取得された他人のID等を第三者に提供する行為等の規制[14]に関して、法制度のあり方も含めた検討が必要と考える。

3.3. まとめ

2009 年度を通してフィッシングサイトの件数は増加し、特に国内ブランドを狙うという傾向が顕著にみられる（1.を参照）。これらの現状に対しては今まで通り動向に関する最新情報を収集し、特に被害にあう国内ブランド間の連携を図ることが当協議会の役割と考えている。

---

[14] いわゆる「犯罪による収益の移転防止に関する法律」では、他人になりすまして銀行口座を利用しまたは第三者をして利用させる目的で行う銀行口座の取引を禁じている（同法第 26 条）。これは、それ自体では直接の問題を生じない口座の取引行為について、犯罪や犯罪収益の隠匿行為の準備として行われることを理由に禁止するものであるが、特に不必要に個人の自由を制約するおそれがあるとはされていない。銀行口座の取引は、それ自体では犯罪性のない行為であるが、犯罪的行為に利用されるおそれが高いため、これを禁止することが正当化されうるとされる。これと同様に、ID 等の不正取得・提供等も犯罪的行為に利用されるおそれが高いため、規制~~禁止~~することも正当化されうるとの考えもある。

（空白）

フィッシング対策協議会　技術・制度検討ワーキンググループ
構成員名簿（改訂版）

（敬称略・順不同）

【主査】

内田 勝也	情報セキュリティ大学院大学

【副主査】

野々下幸治	マカフィー株式会社

【構成員】

白石 知宏	アグスネット株式会社
水村 明博	RSA セキュリティ株式会社
宮本 和明	株式会社 HDE
柿沼 靖雄	エヌ・ティ・ティ・コムウェア株式会社
永塚 淳	エヌ・ティ・ティ・コムウェア株式会社
前田 典彦	株式会社 Kaspersky Labs Japan
石丸 傑	株式会社 Kaspersky Labs Japan
佐藤 克洋	株式会社カービュー
橋本 小月	株式会社カービュー
松本 義和	サイバートラスト株式会社
石田 公孝	有限会社ストーンズインターナショナル
加藤 孝浩	トッパン・フォームズ株式会社
宇井 隆晴	社団法人日本インターネットプロバイダー協会
秋山 卓司	一般社団法人日本電子認証協議会
國米 仁	株式会社ニーモニックセキュリティ
丹京 真一	株式会社日立情報システムズ
上山 達也	ヤフー株式会社
岡本 敏和	ヤフー株式会社

【オブザーバ】

経済産業省商務情報政策局情報セキュリティ政策室

【事務局】

一般社団法人 JPCERT コーディネーションセンター
株式会社三菱総合研究所